SECTION 26. CLASSIFIED NATIONAL SECURITY INFORMATION AND MATERIAL

26-1 DELETED

EFFECTIVE: 02/12/92

26-2 GENERAL CLASSIFICATION INSTRUCTIONS

When material is prepared in the FBI which relates to national security and which meets the criteria of Executive Order 12356, it must be classified and marked in accordance with the provisions of that Order as outlined in this section. Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act or the Privacy Act, if such classification meets the requirements for classification and is accomplished personally and on a document-by-document basis by an individual with original Top Secret classification authority. Information shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information. The Attorney General may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office (ISOO). See ISOO Directive Number One, Section 2001.6 for reporting requirements.

EFFECTIVE: 02/12/92

26-2.1 Authority to Classify, Declassify, Upgrade and Downgrade

(1) Classification may be accomplished through use of a prepared guide which contains instructions for its use and which details the information to be classified, lists the classifying authority, and shows the level of classification and the length of time to remain classified. An example of such a guide is "Classification Guide No. 1" (G-1) regarding Foreign Government Information.

(2) Information may also be classified by incorporating, paraphrasing, restating, or generating in new form information that is already classified. This type of classification, including the use of classification guides, is known as "derivative classification." If previously classified information is used as the basis for classification, the previous markings must be honored and the original source documents must be shown on the "Classified by" line in a manner that will afford retrieval of the source document. Information to be classified which is not classified derivatively may only be classified by an individual having the authority to classify and in accordance with procedures set forth hereinafter.

(3) Authority to classify (or upgrade) material is strictly limited to specifically designated officials and supervisors approved in writing by the Attorney General. Such approval is handled through the Security|Clearances|Unit, Security|Countermeasures| Section,|Intelligence|Division, at FBIHQ.

(4) Agents or support personnel preparing national security material should determine whether there is a basis for classification, the level of classification, and the reasons, but only authorized classifiers may approve such classification (unless it is derivative classification), and only their credential numbers may be used as the classifying authority. In the absence of an authorized classifier, an individual not authorized, such as a relief supervisor, acting on authorized classifier's behalf, may classify material utilizing the authorized classifier's credential number.

(5) Classified material may be downgraded or declassified only by the original classifying authority, by a successor acting in the same capacity, by a supervisory official of either, or by officials delegated such authority in writing by the FBI Security Programs Manager. The successor or supervisory official need not be a classifying authority to downgrade or declassify. Information classified derivatively by classification guides may be downgraded or declassified by Special Agents in Charge and Senior Legal Attaches.

(6) Those individuals in the FBI who have been designated as Original Top Secret Classification Authorities may not redelegate that (or a lesser) classification authority.

(7) The Attorney General of the United States has established the Department Review Committee (DRC) (see 28, Code of Federal Regulations (CFR), Section 17.135) as Department of Justice's (DOJ's) component responsible for the resolution of all issues concerning the implementation and administration of Executive Order 12356 which concerns national security material. The DRC is composed of representatives from various components within DOJ, including the FBI. Classification actions are discussed and voted upon. The DRC may vote to uphold the FBI classification action or may vote that classification is not warranted. The DRC will review and resolve all issues concerning a number of FBI classification actions, which, in part, may relate to:

(a) Administrative appeals of requests for records under the Freedom of Information Act (Title 5, USC, Section 552) and mandatory reviews for declassification when the FBI's proposed denial of information to the requestor is based upon national security concerns;

(b) All classified material which will require the submission of an affidavit or declaration to the Court to justify the nondisclosure of national security information pursuant to Freedom of Information/Privacy Acts (FOI/PA) exemptions or assertion of a "State Secret Claim."

The Document Classification Unit (DCU), Security Section (SS), Information Management Division (IMD), is responsible for liaison with the DRC and should be consulted in connection with any submission of material to the DRC.

EFFECTIVE: 02/12/92

26-2.2 Basis for Classifying Material

EFFECTIVE: 09/26/90

26-2.2.1 Criteria for Classifying Material

For material to be considered for classification, it must meet one or more of the following criteria:

[redacted] b2

EFFECTIVE: 09/26/90

26-2.2.2 Damage Requirement

Information that is determined to concern one or more of the categories in 26-2.2.1 shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

EFFECTIVE: 09/26/90

26-2.2.3 Reason for Classifying Otherwise Unclassifiable Material in Context of Other Material

(1) Certain information which would otherwise be unclassified when standing alone (such as an FD-302, address, or the like), may require classification when combined or associated with other unclassified or classified information. In the context where this normally unclassified information would reveal our investigative interest in certain individuals, organizations, or countries, thereby causing the information now to fall within one of the criteria listed in 26-2.2.1 above, such as an intelligence activity or method, and it meets the criteria in 26-2.2.2, it should be classified.

(2) As a rule, the above basis for classification will be used infrequently inasmuch as the vast majority of classifiable FBI information will be readily identifiable as falling within the categories of (a) foreign government information, (b) intelligence sources, activities, or methods, or (c) foreign relations. Whenever the information is deemed to warrant classification based on the above reason (since it is not readily apparent that it falls within the 26-2.2.1 criteria), a reference must be made to the above reason on the face of the document. This will be accomplished by adding a line below the "Classified by _____" line as follows:

Classified by _____
Reason for Classification: FCIM II, 1-2.2.3
Declassify on: OADR

(3) The above does not apply to situations where the date of the communication, the page number, and otherwise innocuous information warrants classification on the basis that the entire document should be classified to protect the fact that the FBI has an investigation concerning that matter.

EFFECTIVE: 09/26/90

26-2.3 Classification Guidance

Section 26-2.2.1, supra, identified the categories of information that shall be considered for classification. Of the categories listed, those most likely to be encountered by FBI classifiers are:

[redacted] b2

To assist classification authorities in rendering classification determinations concerning this information, the following guidance is supplied:

EFFECTIVE: 09/26/90

26-2.3.1 [redacted]

[redacted] b2

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

5 Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

X Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
X (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
MIOG manual

XXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

26-2.4 Categories (Levels) of Classification

(1) There are three categories or levels of classification: "Top Secret," "Secret," and "Confidential."

(a) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(b) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(c) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(2) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the highest level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

EFFECTIVE: 02/23/84

26-2.5 Duration of Classification

Information shall be classified as long as required by national security consideration. The phrase "Originating Agency's Determination Required," as indicated by the abbreviation "OADR," will be utilized to show the duration of classification, except in those rare instances where there is a clear determination the information can be declassified on a specific date or event.

EFFECTIVE: 02/12/92

26-2.6 Classification Markings

(1) The following markings must be shown on the front page of all classified documents, except teletypes, which will be covered separately:

(a) Classification level ("Top Secret," "Secret," or "Confidential") at the top and bottom of: the front cover, if any; the title page, if any; the first page; the last page; the reverse side of the last page or cover. In addition, each interior page must be marked at the top and bottom according to the highest overall level of classification of the entire document.

(b) The identity of the classifying authority (credential number), classification guide number, or source document (if derivative).

(c) The notation, "Declassify on: Originating Agency's Determination Required" or "OADR," unless there is a clear determination the information can be declassified on a specific date or event. In the vast majority of cases, OADR will apply.

Example: Classified by (credential number)
Declassify on: OADR

(d) In instances where the identity of the originating agency and office are not apparent on the face of a document, the identity of the originating agency must be placed below the "Classified by" line (ISOO Dir. No. 1, Section 2001.5 (c)). This situation would occur most frequently at FBIHQ in classifying other Government agency information, such as an INS record. The FBI would be considered the originating agency for the classification decision in this instance and would have to be so noted. If this addition warrants classification, the portion should be marked accordingly.

(2) An ISOO booklet entitled "Marking," which is available from the Information Systems Security Unit, Security Countermeasures Section, Intelligence Division, FBIHQ, contains detailed, yet simple, instructions and examples on marking classified documents.

(3) When material is classified solely because of other agency data, it must be appropriately marked to correspond with the other agency's markings.

(4) When classified material is downgraded, upgraded or

declassified, a line will be drawn through the previous level of classification and related markings, and the new level, along with "upgraded," "downgraded" or "declassified," noted adjacent thereto, together with the date and credential number of the declassifier or classification authority, whichever is appropriate.

EFFECTIVE: 10/14/93

26-2.6.1 Internal Documents Prior to 1974

Prior to 1974, classification markings were not included on classifiable internal FBI documents. All such documents, when subject to disclosure, must be reviewed and appropriately marked for classification.

EFFECTIVE: 03/23/92

26-2.6.2 Marking of Separate Documents and Transmittal Documents

FBI reports have two parts, the cover page(s) and the report itself. For classification purposes, each part must be considered separately and marked appropriately. There will be instances when the cover page(s) is classified but not the report, and vice versa. Each part must indicate the level of classification, identity of the classifying officer, declassification date, etc. Similarly, a transmittal document, such as a cover letter/airtel to an LHM, a form letter, or a routing slip must be considered separately and marked accordingly. An unclassified transmittal document must be marked top and bottom of the front page with the highest classification level of any information transmitted by it. It must also be marked with an appropriate instruction indicating it is unclassified when separated from classified enclosure(s). If the transmittal document itself contains classified information, mark it as required for all other classified information, except:

(1) conspicuously mark the top and bottom of the front page of the transmittal document with the highest classification level of any information contained in the transmittal document or its enclosures; and

(2) mark the transmittal document with an appropriate

instruction indicating its overall classification level when separated from its enclosures.

EFFECTIVE: 03/23/92

26-2.6.3 Marking Separate Paragraphs (See MIOG, Part II, 16-18.8.2(2), 16-18.8.13(5); Correspondence Guide-HQ, 1-4.1(3); Correspondence Guide-Field, 1-21.1(3); FCIM, Part II, 1-2.6.3.)

(1) Whenever portions of classified material require different levels of classification, then each paragraph or portion must be marked to show its classification or that it is unclassified. (A "portion" includes the title or subject, as well as a paragraph, sentence or word of a communication.) In marking individual portions, the appropriate marking ("Top Secret," "Secret," "Confidential," or "Unclassified") should be typed in parentheses immediately following the portion in question. Abbreviations may be used (TS, S, C, or U). An introductory caveat, such as "This document is classified 'Secret' in its entirety, unless otherwise noted," may be used when the majority of the document is at the same level, thereby requiring only the portions that differ to be marked. A similar statement should be used to show the document is classified in its entirety, if that is the case. (See (2) below.)

(2) The FBINET subnetwork is authorized to process up to and including SECRET/collateral data. Under no circumstance may TOP SECRET (TS) or Sensitive Compartmented Information (SCI) be processed by FBINET, or entered into any Automated Information System (AIS) which is accessed by FBINET. AISs which utilize the FBINET subnetwork include: the Field Office Information Management System (FOIMS); the Resource Management System (RMS); the Criminal Law Enforcement Application (CLEA); the Criminal Law Enforcement System (CLES); the Investigative Support Information System (ISIS); the Uniform Crime Reporting System (UCRS); the Legal Counsel Information System (LCIS); and, the Training Division Support System (TDSS). To ensure compliance with this restriction, all correspondence containing TS or SCI data will be "portion marked" to show specific classification levels (i.e., title, each paragraph, etc.) Although a document may have an overall classification of TS and/or SCI, frequently the information to be entered into the AIS may actually be classifiable at a lower level. Portion marking will allow for that information which is classified as SECRET/collateral or below (if any) to be entered

into AISs accessed by the FBINET subnetwork. Under no circumstances may SCI, regardless of classification level, be processed on the FBINET subnetwork or entered into any AIS accessed by the FBINET subnetwork. However, SCI material can be appropriately downgraded, based on the approval of the originating agency, to the SECRET/CONFIDENTIAL collateral level through written summaries, etc., so it may be processed via FBINET. (Also see MIOG, Part II, Section 26-2.6.3(1).)

EFFECTIVE: 11/25/94

26-2.6.4 Marking Teletypes

Teletypes are marked with the classification level ("UNCLAS" or "UNCLAS E F T O," if unclassified) preceding the text on the first page and at the top of each succeeding page. The abbreviation "C BY _____; DECL: OADR" will be utilized at the end of the message on teletypes.

EFFECTIVE: 03/23/92

26-2.6.5 Marking Derivatively Classified Documents Being Disseminated Outside the FBI

When documents are being disseminated outside the FBI and have been classified derivatively, they should be treated as follows:

(1) If the derivative source is a single document, mark the outgoing copies "Classified by Derivative Source," and identify the source document on all FBI copies.

(2) If the derivative source is multiple documents or sources, mark the outgoing copies "Classified by Multiple Sources," and identify the multiple sources on all FBI copies.

EFFECTIVE: 03/23/92

26-2.7 Material With Different Classification Levels or Declassification Dates

When classified material consists of two or more items of information which bear different classification levels or declassification dates, the following guidelines apply:

(1) Material containing different levels of classified information must be classified at the level of the highest classified component.

(2) Material containing different declassification dates must be marked with the most distant declassification date.

EFFECTIVE: 02/12/92

26-3 SPECIAL CLASSIFICATION INSTRUCTIONS

The procedures set forth above will not cover all situations involving classification matters. It is emphasized that the objective is to protect national security material in our files in a practical and reasonable manner. In connection with any problems not covered in these instructions which cannot be handled locally, the Security|Clearances|Unit, Security|Countermeasures|Section, |Intelligence|Division, should be consulted. Following are some special classification instructions representing classification decisions that have already been made and should be adhered to.

EFFECTIVE: 02/12/92

||26-3.1 Classification of Notes

(1) When a note containing classified information is affixed to a communication that is unclassified, they should be treated as a single document and marked accordingly. In actual practice, this would mean that the original communication going to the field would be unmarked and would bear no reference to any classified material, whereas the FBIHQ copies containing the note would be classified and marked accordingly. The classified document would either have to be portion-marked or contain a caveat to the effect that all portions are unclassified unless otherwise noted. This caveat should not appear on the original unclassified document.

(2) When classified enclosures are added to the above example, each package should be treated separately. The markings on each transmittal letter would be handled in accordance with instructions set forth in 26-2.6.2 above.

(3) For variations of the above, such as when the original and note are both classified, but at different levels, the same logic would apply, i.e., they would be treated as a single document. The reasoning behind treating the note and communication as a single document is because, generally, they are both prepared at the same time by the same person and are not intended to be utilized separately. In the event a note is added to a document at a later time by someone other than the originator of the document, that person has the responsibility to ensure proper classification procedures are followed with respect to the note.

EFFECTIVE: 02/23/84

26-3.2 Classification of Addenda and Attachments to Documents

(1) The intent behind Executive Order 12356 is that the individual generating information meeting the criteria for classification has the responsibility for ensuring that it is properly classified. In the situation where addenda are added to a communication by someone other than the originator, that person has the responsibility of ensuring that this information is properly classified. Even though an addendum is not likely to be used separately, it should still be marked as separate document, notwithstanding the fact that it might be numbered as if it were a single document. The key element is that it represents another individual's thought, and that individual has the responsibility to classify it. It would, therefore, be possible for a memorandum to be classified "Secret" in its entirety, one addendum to be "Unclassified," and another to be classified in part.

(2) Consideration should be given always to the possibility that an otherwise unclassified addendum might warrant classification by virtue of it being linked with a classified memorandum. If the originator of the memorandum determines an addendum prepared by another individual should have been classified, he/she has the prerogative to classify it.

(3) Since each component is to be marked as a separate

document, a notation on the first page of a memorandum, such as "All information contained herein is classified "Secret" unless otherwise noted," would apply only to the memorandum and not to any attachments or addenda. Likewise, the "Secret" markings at the top and bottom of each page of the memorandum should not be applied to the attachments or addenda unless they also are "Secret." They should be marked at the appropriate level of classification of the newly created document(s).

(4) In situations where memoranda with addenda attached are being reviewed for classification, such as pursuant to a Freedom of Information Act request, each part should be treated as a separate document to avoid confusion and enhance uniformity.

EFFECTIVE: 02/23/84

26-3.3

[redacted]

b2

EFFECTIVE: 02/23/84

26-3.4

[redacted]

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

3 Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

X Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☒ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
MIOG manual

XXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

26-3.12 [redacted]

[redacted]

b2

EFFECTIVE: 11/21/89

26-3.13 CIA - Classification of Covert Operations

[redacted]

b3
b7E
CIA

EFFECTIVE: 11/21/89

26-4 ACCESS TO CLASSIFIED INFORMATION BY INDIVIDUALS HAVING OFFICIAL CLEARANCES

All FBI employees are cleared for access to classified national security material up to and including "Top Secret" on a strict need-to-know basis. No individual is to be permitted access to classified or classifiable material appearing in the files of the FBI unless they have been afforded official clearance for such access and have a need to know. It will be incumbent upon each FBI employee permitting such access to be assured the required clearance has been obtained. Questions as to whether an individual is cleared for access to national security material which cannot be resolved locally are to be referred to the Security Programs Manager at FBIHQ. Any instance of unauthorized access or attempted unauthorized access to national security material should be promptly reported to Director, FBI, Attention: Security Programs Manager.

EFFECTIVE: 05/26/89

26-4.1 Inadvertent Unauthorized Access to National Security Information

(1) In cases where national security information has been disclosed to an individual who has not had appropriate clearance(s) or has inadvertently had unauthorized access to national security information, that individual, once interviewed and briefed as to his/her responsibility and obligation not to disclose national security information, is to sign and date the Inadvertent Disclosure Statement, Form FD-722. This form provides an affirmation suitable for execution by any individual who has inadvertently obtained national security information. The form is to be witnessed by the FBI representative present. An individual who does not wish to sign the FD-722 should be briefed as to its contents. The reason for refusal should be noted on the form, which will then be appropriately witnessed.

(2) The original and one copy of the executed FD-722 are to be forwarded to FBIHQ, Attention: Security Programs Manager, as enclosures to a self-explanatory cover memorandum.

EFFECTIVE: 05/26/89

26-5 STORAGE OF CLASSIFIED MATERIAL (See MIOG, Part I, 261-2 (3)(a), (4)(a); Part II, 16-7.2.6 (9)(g), 35-9.4.9; NFIPM, Part 1, 8-5; Correspondence Guide - Field, 1-21.7.)

Introduction

Classified material, including classified information on storage media used by typewriters, word processors, or remote terminal equipment, shall be protected at all times. Whenever classified material is not under the personal control (observable and sufficiently close to prevent unauthorized access) of an authorized and appropriately cleared person, whether during or outside of working hours, it will be guarded or stored in a locked security container, as described herein, or a secure storage room, as described in Section 26-5.2. FBI employees are responsible for the protection and storage of classified information and material in

their custody. It is the responsibility of the holder of classified material to ensure that material is properly protected and, through verification of clearance/access and need to know, not provided to an individual who is neither authorized nor cleared to receive it. Storage equipment not functioning in a normal manner shall be immediately reported to the appropriate Security Countermeasures Program Manager or Security Officer for corrective action. The adjustment or repair of security equipment will be accomplished only by trained personnel. Until repairs have been made, defective equipment shall not be used to safeguard classified items.

EFFECTIVE: 09/09/97

26-5.1 Storage of "Top Secret" Material (See MIOG, Part II, 35-9.4.9; NFIPM, Part 1, 8-5.1; MAOP, Part II, 2-4.3.1 (1)(k); Correspondence Guide - Field, 1-21.7.)

"Top Secret" material must be stored in a General Services Administration (GSA)-approved [redacted] b2

[redacted] Resident agencies, Legal Attache offices, and field office and FBIHQ off-site facilities are not authorized to process or maintain "Top Secret" material or information unless approved in writing by the Security Programs Manager, National Security Division, FBIHQ. All "Top Secret" material must be segregated from general files, whether pending or closed, and stored in approved containers. Only FBI employees and other specified personnel with a verified security clearance and a "need to know" shall have access to "Top Secret" material.

EFFECTIVE: 09/09/97

26-5.2 Storage of "Secret" and "Confidential" Material
(See MIOG, Part II, 26-5, 35-9.4.9; NFIPM, Part 1, 8-5.2; Correspondence Guide - Field, 1-21.7.)

"Secret" and "Confidential" material must be stored in GSA-approved security containers having GSA-approved, [redacted] "Secret" and "Confidential" information may be openly stored (not in a GSA-approved safe) in a secure storage room which has been approved in accordance with specific Department of Justice requirements. Although similar in construction, these secure facilities are not Sensitive Compartmented Information Facilities (SCIFs) and are not approved for the storage of Sensitive Compartmented Information (SCI) at any level of classification. The approval for a secure storage room for the open storage of classified material must be obtained in writing from the Security Programs Manager, National Security Division, FBIHQ. Access to "Secret" and "Confidential" material is limited to appropriate personnel with a verified security clearance and a need to know.

EFFECTIVE: 09/09/97

26-5.2.1 Storage of "Sensitive Compartmented Information (SCI)"
(See NFIPM, Part 1, 8-5.2.1; MAOP, Part II, 2-4.3.1 (1)(k); Correspondence Guide - Field, 1-21.7.)

(1) SCI is classified information (Confidential, Secret, or Top Secret) concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence (DCI). SCI is sometimes referred to as "codeword" material.

(2) The Director of Central Intelligence Directive (DCID) 1/21, entitled "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)," requires that all SCI be stored, processed, or discussed within an accredited SCIF. Accreditation is the formal affirmation that the proposed facility meets applicable physical security standards as set forth in DCID 1/21. The accreditation for a SCIF must be obtained in writing from the Security Programs Manager, FBIHQ. For further information regarding the handling of SCI, contact a representative of the

Security Countermeasures Section, National Security Division.

EFFECTIVE: 09/09/97

26-5.3 Removal of Classified Material to Residence

(1) Employees may not remove classified material from official premises to their residence during nonworking hours without approval from the Director, the FBIHQ Security Programs Manager (SPM), the SAC for FBI field offices, or the appropriate Assistant Director at FBIHQ. In every instance of approval, the material removed must remain in the personal control of the authorized employee at all times unless a safe and an alarm are installed in the residence by the FBI. Before installing any such equipment in a residence, the SPM at FBIHQ should be contacted for guidance.

(2) Control files are to be established, both at FBIHQ and in the field offices, to document those requests to remove classified material to an employee's residence. The file will include the date and duration of the request, the justification, signature approval granting or denying the request, the name of the authorized individual, and a description of the classified material being charged out.

(3) This authority does not apply to Legats.

EFFECTIVE: 07/23/90

26-5.4 Proper Use and Changing of Lock Combinations and Disposal of Combination Locks/Security Equipment (see also Part II, Section 16-7.2.6(9) of this manual)

(1) Except as otherwise noted, it shall be the responsibility of the supervisory or management official using or overseeing the use of security equipment that appropriate administrative controls are in place to ensure compliance with all requirements set forth herein.

[redacted] b2

[redacted]

b2

(4) Records of combinations must be classified no lower than the highest category of classified material stored in the involved security equipment and must be protected in accordance with established guidelines addressing the handling and storage of NSI.

(a) A central Combination Record File is to be established in each division, Legat, regional computer center, or other off-site Bureau component, and combinations for all security containers used to store classified material are to be maintained in this file. This file is to be securely maintained in a fashion commensurate with the highest classification level of any document in the file.

(b) Standard Form (SF) 700, entitled "Security Container Information," is to be completed each time a combination is changed. This is a three-part, self-explanatory form. Upon completion, Part 1 is to be affixed to the inside of the affected vault, safe, door, or security container. Part 2A is to be completed and sealed inside Part 2, an envelope designed for this purpose, which in turn, is to be maintained in the central Combination Record File.

(c) It shall be the responsibility of the individual Legats and Security Officers to ensure all combination records for all equipment used to store classified material are properly classified and maintained.

(d) Written records of combinations must be maintained only as described herein. They are not to be retained in either "coded" or "uncoded" form on the person of any employee or other individual having access to the affected security equipment, nor are they to be recorded in any form on index cards, calendars,

notebooks, etc., which are not being maintained in compliance with established guidelines set forth herein for the protection of NSI.

(5) Combinations shall be changed only by persons having the appropriate security clearance and/or special access, if applicable, for the type of classified material stored in the security container. The same shall apply to the Security Officer (SO), Alternate Security Officer (ASO), or any other individual designated to accompany this person. Clearances/special accesses may be verified by SOs or other designated individuals through the office of the Security Programs Manager, FBIHQ, Extension [redacted]

b2

(a) In field offices, resident agencies, and off site locations associated with a field office, all combination changes are to be made by a Technically Trained Agent (TTA) and under the general direction of the field office SO or ASO. A responsible employee designated by the SAC or ASAC and familiar with security requirements governing the protection of NSI should also be present when the combination is changed.

(b) In Legats, all combination changes are to be made by the Legat, Assistant Legat, or other office personnel certified by the Engineering Section (ES), Technical Services Division (TSD). A responsible employee designated by the Legat or Assistant Legat and familiar with the security requirements governing the protection of NSI should also be present when the combination is changed.

(c) In regional computer centers or other FBI components not specifically associated with a field or FBIHQ division, all combination changes are to be made by the SO, ASO, or other personnel certified by ES, TSD. A responsible employee designated by the administrator of that component or his/her senior assistant and familiar with the security requirements governing the protection of NSI should also be present when the combination is changed.

(d) For all FBIHQ divisions, all combination changes are to be made by technically trained Bureau personnel certified by ES, TSD, and under the general direction of the division SO or ASO. A responsible division employee designated by no less than at the Unit Chief level and familiar with security requirements governing the protection of NSI should also be present when the combination is changed.

(e) The same combination will not intentionally be used for more than one lock in any field or FBIHQ division, Legat,

regional computer center, or other off-site location. In selecting combination numbers, multiples of five, simple ascending or descending arithmetical series, personal data (such as birthdates), and serial numbers, must be avoided. Only numbers that are widely separated may be used. The last number of a built-in combination lock shall not be set between 90 and 20. To prevent a lockout, a new combination is to be tried at least three consecutive times before closing the door or drawer.

(f) When security equipment is taken out of service, it shall be inspected to ensure no classified information or other FBI data remains, and the built-in combination lock shall be reset to the standard combination 50-25-50. Combination padlocks shall be reset to the standard combination 10-20-30.

(6) To properly secure a combination lock, the dial must be turned four or more complete revolutions in the same direction. Spinning the dial quickly is to be avoided as it shortens the life span of the tumblers/wheels, may cause other damage to the lock, and may not properly secure the lock. Combination locks are not to be left in an unsecured condition and the combination numbers are not to be left predialed to facilitate easy opening after an absence, as such a practice defeats the security protection of a combination-locked repository.

EFFECTIVE: 07/23/90

26-6 CONTROL FORM FOR TOP SECRET (TS) - SENSITIVE COMPARTMENTED INFORMATION (SCI) - NON-SCI CODE WORD MATERIAL - FD-501 - FD-502

Accountability, receipting and control of "Top Secret," Sensitive Compartmented Information (SCI), and Non-SCI Code Word Material within a field office or within FBIHQ is controlled through the use of the FBI "Control Form for Top Secret (TS), Sensitive Compartmented Information (SCI), and Non-SCI Code Word Material," FD-501. An original of an FD-501 will be attached to each copy of the material and the copy of FD-501 will be retained by the Security Officer to ensure he/she is aware of the location of the material at all times. "Top Secret" and/or Sensitive Compartmented Information being transmitted between field offices and/or FBIHQ or to outside agencies is controlled through the use of the "Receipt for Top Secret (TS) - Sensitive Compartmented Information (SCI), and Non-SCI Code Word Material," FD-502, which is attached to the material while being

transmitted. The recipient of the material will sign and return the original FD-502 to FBIHQ, Room 5991, or the Security Officer of the transmitting field office.

EFFECTIVE: 01/18/91

26-7 TRANSMITTAL OF CLASSIFIED MATERIAL

EFFECTIVE: 01/18/91

26-7.1 Within Field Offices

Material classified "Top Secret" or containing Sensitive Compartmented Information must be hand carried in an envelope within field offices. Material classified "Secret" or "Confidential" may be routed by messenger within field offices but must be in a messenger envelope except when records processing procedures such as indexing, serializing, filing, etc., are handled by OSM personnel within a field office.

EFFECTIVE: 01/18/91

26-7.2 Between Field Offices and/or Resident Agencies, Outside Agencies and FBIHQ (See MIOG, Part II, 35-9.4.14; MAOP, Part II, 2-2.2.2(1)(d); Correspondence Guide-FBIHQ, 1-4.5(4); Correspondence Guide-Field, 1-21.5(2); and National Foreign Intelligence Program Manual, Part I, 8-7.2.)

Material classified "Top Secret" or containing Sensitive Compartmented Information may only be transmitted between field offices and/or resident agencies, outside agencies and FBIHQ by secure teletype, by FBI courier designated by the SAC or Security Programs Manager or by Defense Courier Service (DCS). (See Part II, 26-6 above for use of control forms.) Material classified "Secret" or "Confidential" must be enclosed in opaque sealed envelopes or in opaque sealed boxes and may be transmitted by United States Postal Service (USPS) Registered Return Receipt, USPS Express Mail, or Federal Express (FedEx) between FBI offices within the United States and Puerto Rico. FedEx does not deliver to post office boxes. To

ensure direct delivery to the addressee, the "Waiver of Signature and Indemnity" block on the|USPS|Express Mail Label, 11-B, and the "Release Signature" block on the|FedEx|Airbill Label may NOT be executed under any circumstances. All "Confidential" and "Secret" express|mail|shipments should be|prepared by FBI employees and hand-delivered directly to a FedEx|representative or a|USPS facility|representative. The use of|collection|boxes is prohibited. For marking of transmittal documents, refer to 26-2.6.2 above.

EFFECTIVE: 06/06/96

26-7.3 Defense Courier Service (DCS); FBI Courier

"Top Secret" or Sensitive Compartmented Information which cannot be sent by secure teletype between field offices and/or FBIHQ must be transmitted by DCS or an FBI courier designated by the SAC or Security Programs Manager. "Top Secret" or Sensitive Compartmented Information transmitted between field offices and resident agencies or to outside agencies within the field office territory must be transmitted by an FBI employee designated as a courier by the SAC.

EFFECTIVE: 01/18/91

26-7.4 Wrapping Classified Material

"Top Secret" or Sensitive Compartmented Information transmitted by|DCS|must be wrapped in accordance with packing standards set forth in Appendix C,|DCS|Administrations and Operations Regulations. "Top Secret" or Sensitive Compartmented Information transmitted by FBI employees designated couriers by the SAC and "Secret" and "Confidential" material sent by registered mail must be enclosed in opaque sealed envelopes where size permits or in opaque sealed boxes in accordance with instructions set forth in Title 28, Code of Federal Regulations, Part 17.104.

EFFECTIVE: 07/23/90

26-8 MATERIAL CLASSIFIED UNDER PRIOR ORDERS

When incorporating information classified under previous Executive orders into a new document and no specific declassification date was indicated thereon, or if it was marked "indefinite," then a date for declassification must be shown or "OADR" (Originating Agency's Determination Required).

EFFECTIVE: 07/23/90

26-9 ATOMIC ENERGY MATERIAL MARKINGS

Additional warning markings "Restricted Data" and "Formerly Restricted Data" are used in connection with atomic energy-type material. These markings must be included on the first page when such classified material is set forth in FBI-originated documents.

EFFECTIVE: 07/23/90

26-10 SENSITIVE COMPARTMENTED INFORMATION (SCI)

EFFECTIVE: 07/23/90

26-10.1 Definition of SCI

(1) SCI access is regulated by the Director of Central Intelligence Directive (DCID) No. 1/14. SCI is all information and material requiring special U.S. Intelligence Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. These special Community controls are formal systems of restricted access established to protect the sensitive aspects of foreign intelligence programs. DCID No. 1/14 establishes minimum personnel security standards and procedures which govern eligibility for access to SCI.

(2) SCI security control systems depend upon distinctive markings and restricted handling of material, stricter personnel security processing for access, and holding SCI material in "Control Centers" with physical and procedural barriers to preclude access by

those who have not been formally approved. The SCI control systems provide an organized program for predetermining a generalized "need-to-know" regarding specific categories of intelligence and/or the sources and methods employed in their collection.

(3) SCI systems cover activities and information of extraordinary sensitivity and fragility from a security standpoint. They serve to restrict access to the protected information to persons who have a clearly established "need-to-know." "Need-to-know" exists only when access to SCI is essential to a person for the performance of official duties. Personnel granted access to SCI must meet rigorous and stringent personnel security criteria. Individuals cleared for Top Secret information are not automatically eligible for access to SCI.

EFFECTIVE: 07/23/90

| 26-10.2 SCI Access |(See MIOG, Part II, 35-9.2.)|

(1) Persons indoctrinated for SCI accept certain responsibilities and restrictions in a most explicit way. As a condition of access, an individual signs a nondisclosure agreement which is a contractual agreement between the government and the individual. This agreement should be read carefully before signing, because it states obligations imposed upon the individual and the government. Willful disclosure of SCI to unauthorized individuals constitutes criminal or administrative offenses which may result in prosecution or administrative action.

(2) Access to SCI will be granted when the "need-to-know" is established, eligibility determined, SCI nondisclosure agreement (Form|4414)|signed, and indoctrination completed.

EFFECTIVE: 04/10/96

26-10.2.1 FBIHQ/Field Office/Legat Personnel Security Access Certification Procedures

DCID No. 1/14 sets forth the minimum personnel security standards and procedures governing eligibility for access to SCI. The purpose of this Directive is to enhance the security protection of SCI through the application of minimum security standards, procedures, and continuing security programs, and to facilitate the security certification process among government departments and agencies.

Accordingly, the following procedures will be followed by FBI Headquarters (FBIHQ) and field divisions when access to SCI is required:

(1) A written communication requesting SCI access shall be directed to the |National Security Division,| Attention: Security Programs Manager (SPM). |The communication should utilize the employee's 67 file number.| The communication shall be captioned as follows:

"ACCESS TO SCI, _____ DIVISION."

The following information shall be included for each individual for whom access is being requested:

A. Bureau name

B. Position

C. Social Security Account Number

D. Supervisor's written certification of employee's "need-to-know"

E. SCI access or accesses requested

|(2)|The division Security Officer will be advised in writing of access approval. The written communication will authorize the Security Officer to conduct a formal briefing and security indoctrination in accordance with the minimum requirements set forth in "Annex C," DCID No. 1/14, page|2.|

|(3)Form 4414, "Sensitive Compartmented Information Nondisclosure Agreement,"|should be executed prior to the formal briefing and, thereafter, forwarded to the SPM.

In emergency cases where immediate access is required, the division Security Officer may, by secure telephone, provide the aforementioned information to the Supervisory Special Agent managing the SCI Program for the SPM, followed by a routine teletype confirming that information. FBIHQ will expedite access approval by secure telephone. If an exception to the investigative requirements is granted to facilitate an immediate interim access, the prescribed investigation shall, nevertheless, go forward.

For TURK purposes, these matters will be handled under the 67E classification, "Reinvestigation of FBI Personnel."

EFFECTIVE: 04/10/96

26-10.2.2 |Deleted|

EFFECTIVE: 04/10/96

26-10.2.3 Denial/Revocation

A denial or revocation of access to SCI shall be in accordance with procedures established in "Annex B" to DCID No. 1/14, which is titled "Appeals." For purposes of denial or revocation, the determination authority for the FBI shall be the SPM. The final appeal authority remains with the Director of the FBI or his designated representative at the Associate Deputy Director level.

EFFECTIVE: 12/10/91

26-10.2.4 Termination/Debriefing

SCI access must be terminated when an employee no longer has a "need-to-know." This can be occasioned by position transfer, retirement, resignation, suspension, maternity leave, etc. At this time, the Security Officer will debrief the employee in accordance with the guidelines provided in "Annex C," DCID No. 1/14.

EFFECTIVE: 12/10/91

26-10.2.5 Exceptions to DCID No. 1/14

Exceptions to the minimum standards as set forth in DCID No. 1/14 may be granted only by the Senior Official of the Intelligence Community (SOIC). For the purposes of DCID No. 1/14, an SOIC is defined as a head of an organization within the Intelligence Community, as defined by Executive Order (EO) 12333, or their designated representative. EO 12333 defines the intelligence activities of the United States and specifically states the intelligence element of the FBI is part of the Intelligence Community. The SOIC for the FBI is the Director, who specifically delegated the responsibility for the administration of SCI policy and procedures for the FBI to the SPM.

EFFECTIVE: 12/10/91

26-10.2.6 Access to Sensitive Compartmented Information (SCI) Recertification Procedures, Reinvestigation of FBI Personnel (See MIOG, Part I, 67-18(1)(e).)

The SCI access mandatory recertification process is to be conducted annually by each Security Countermeasures Programs Manager (SCMPM) or his/her designee.

(1) The Security Programs Manager (SPM), FBIHQ, will forward to each field office and FBIHQ division/office a list of designated employees with SCI access on or about May 1 of each calendar year.

(2) The list will contain each employee's name, social security number, SCI access, briefing date, debriefing date, and

comment section.

(3) Each SCMPM will review, verify, and certify the identifiable information pertaining to each employee.

(a) When a determination is made to continue with the SCI access, the SCMPM is required to provide a succinct statement justifying the continuation of the SCI access.

(b) In those instances when the SCI access continuance cannot be fully justified, then steps must be initiated to debrief the employee immediately.

(c) When an employee is debriefed, a blank copy each of Form 4414, entitled "Sensitive Compartmented Information Nondisclosure Agreement," and SF-312, entitled "Classified Information Nondisclosure Agreement," is to be given to each debriefed employee. Both forms are to serve as a reminder of the consequences and statutory requirements for protecting national security information.

(4) The SCMPM is required to maintain a copy of the SCI access recertification list from year to year.

(a) Upon receipt of the current year's list of employees, the previous year's list is to be destroyed.

(b) The list of employees is to be maintained in accordance with established procedures for handling and storing Sensitive Compartmented Information.

(5) The recertification list, with appropriate comments and debriefing form (Form 4414), should be returned to the SPM within 60 calendar days from the date of the SPM's cover communication.

(6) The SCMPM or his/her designee is to ensure those employees whose SCI access is no longer required are debriefed routinely.

(7) Whenever an employee's conduct is no longer commensurate with DCID Number 1/14, Executive Order 10450, and/or the employee's misconduct impacts on his/her trustworthiness, the SCMPM is required to conduct a personnel security interview with the employee and notify the SPM, FBIHQ, providing a recommendation as to whether the employee's SCI access should be suspended, denied, or revoked pending the SPM's final adjudicative decision.

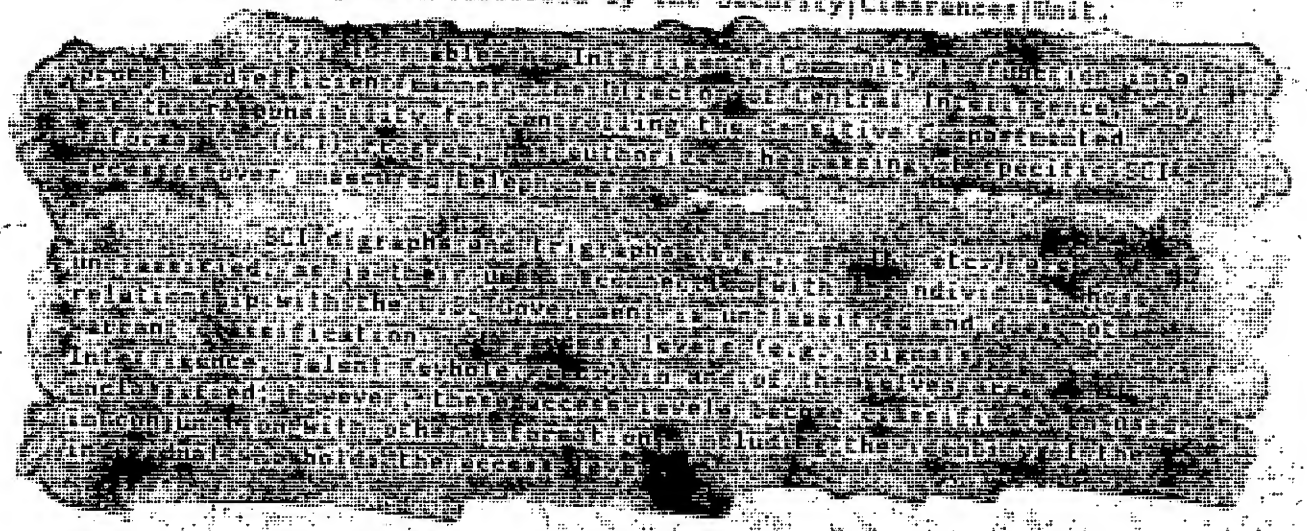
EFFECTIVE: 10/12/93

26-11 CERTIFICATION OF CLEARANCES

EFFECTIVE: 12/10/91

26-11.1 Visits to Other Agencies by Current Employees

(1) The Security|Clearances|Unit, FBIHQ will pass/certify all clearances for FBIHQ personnel when required for visits to other agencies. Upon request from the field Security Officer, the Security|Clearances|Unit will also pass/certify clearances for field office personnel when required for visits to other agencies. All requests should include: The level of clearance needed at the meeting; point-of-contact and telephone number; date(s) of visit; and reason for visit. Field Security Officers have the authority to pass/certify employee's security clearances in that field office to other agencies. Frequently, however, many other Government agencies and private sector organizations will not accept security clearances unless they are passed/certified by the Security|Clearances|Unit.



EFFECTIVE: 12/10/91

26-11.2 Converting FBI Clearances to Clearances for New Employer

(1) When current or former FBI employees apply for positions with other Federal Government agencies or with private industry which require security clearances, inquiries concerning their FBI security clearances should be directed to the Security|Clearances| Unit|(SCU),|Security|Countermeasures|Section,|Intelligence|Division. |SCU|personnel should request that all such inquiries be made in writing, to allow for a proper review of the employee's personnel file, and any other file that would be pertinent to the request, such as an Administrative Inquiry Matter.

(2) Executive Order (EO) 10450, "Security Requirements for Government Employment," mandates, in Section 3(a), that Government agencies must, at a minimum, make written inquiry to former employers, among other things, when seeking to hire an individual. Section 8 of this Order specifically details the type of information these written inquiries are designed to obtain, all of which is aimed toward determining the individual's suitability for Federal employment.

(3) DOJ Order 2600.3A, "Requirements for Safeguarding Classified Information and Materials Released to Industry in Connection With Contracts or Grants," and the Department of Defense (DOD) Industrial Security Manual (Section III, paragraph 27), both of which govern the FBI's relationship with private industry, require a similar written inquiry to former employers, as specified above, when attempting to convert a former Government clearance.

(4) In order for the FBI, as a current or former employer, to conform to the requirements in EO 10450, DOJ Order 2600.3A, and DOD Industrial Security Manual,|SCU|personnel will review all pertinent files concerning the employee, specifically to include personnel and Administrative Inquiry files, and furnish the requester any information deemed pertinent (to include derogatory information) to assist in the proper adjudication of the clearance matter.

EFFECTIVE: 02/12/92

26-12 SPECIAL CONTROL MARKINGS FOR SENSITIVE INTELLIGENCE SOURCES AND METHODS AND FOR FOREIGN INTELLIGENCE MATERIAL

EFFECTIVE: 02/12/92

26-12.1 Warning Notice - Sensitive Intelligence Sources and Methods Involved (WNINTEL)

(1) In addition to instructions relating to dissemination of classified material set forth in the National Security Council Directive of May 17, 1972 (classified information or material originated in one department shall not be disseminated outside any other department to which it has been made available without the consent of the originating department - known as the "third agency rule"), the Directive also requires that all information and material relating to sensitive intelligence sources and methods be prominently marked "WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED" (WNINTEL). The Directive instructs that material so marked may not be disseminated in any manner outside authorized channels without permission of the originating department and an assessment by the senior intelligence officer in the disseminating department of the potential risk to the national security and to the intelligence sources and methods involved.

[redacted] b2

(3) For FBI purposes, the marking "WNINTEL" will be utilized only in connection with Sensitive Compartmented Information (SCI) or uniquely sensitive information.

EFFECTIVE: 02/12/92

26-12.2 Foreign Intelligence Material

In addition to level of classification markings ("Top Secret," "Secret," and "Confidential") and WNINTEL markings, the following additional markings may be used on foreign intelligence when, in the opinion of the originating organization, extraordinary circumstances require further restrictions on dissemination of foreign intelligence:

(1) DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (ORCON) - May not be disseminated outside of the Headquarters of the receiving agency in any form, even extracted or paraphrased, without permission of originator.

(2) NFIB DEPARTMENTS ONLY (NFIBONLY) - May not be disseminated to an organization not represented on the National Foreign Intelligence Board without permission of the originator.

(3) NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS (NOCONTRACT) - May not be disseminated to contractors or contractor-consultants without permission of originator.

(4) CAUTION - PROPRIETARY INFORMATION INVOLVED (PROPIN) - Recipients shall take every precaution to ensure the information is not used to the detriment of the source.

(5) NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN) - May not be released in any form to foreign governments, foreign nationals or non-U.S. citizens without permission of the originator.

EFFECTIVE: 02/12/92

26-13 UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION

Department of Justice and FBI regulations provide for disciplinary action for employees who violate provisions of Executive Order 12356 and stringent administrative action may be taken against any employee determined to have been knowingly responsible for unauthorized disclosure of classified national security material. Whenever a violation of criminal statutes may be involved, prosecution may also be instituted. (See MIOG, Part II, Section 26-4.1.) The National Foreign Intelligence Program Manual (NFIPM), Appendix, 4-1.1, states in part that anyone who willfully delivers or, through gross negligence, loses any defense information is liable to $10,000 fine or imprisonment for not more than ten years, or both.

EFFECTIVE: 02/14/97

26-13.1 Loss or Possible Compromise of Classified Information (See MIOG, Part I, 261-2(3)(b), II, 26-13.2, 26-13.3 (4); MAOP, Part II, 2-4.3.8(1)(a), 6-7.5(2)(h).3; FCIM, Part I, 65-8.)

Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to FBIHQ, Attention: Security Programs Manager (SPM), and the field office Security Countermeasures Program Manager. When appropriate, the SPM will coordinate with the relevant substantive FCI entities within the National Security Division to ensure compliance with the instructions set forth in the FCIM, Part I, Section 65, "Espionage," Section 65-3, "FBIHQ Policy." In addition, the SPM will notify the agency that originated the information of the loss or possible compromise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise pursuant to guidelines set forth in Title 32, Code of Federal Regulations (CFR), Part 2001, Section 2001.47, as follows:

"(a) Initiation of Damage Assessments. An agency head shall initiate a damage assessment whenever there has been a compromise of classified information originated by that agency that, in his or her judgment, can reasonably be expected to cause damage to the national security. Compromises may occur through espionage,

unauthorized disclosures to the press or other members of the public, unauthorized sales, publication of books and treatises, the known loss of classified information or equipment to foreign powers, or through various other circumstances.

"(b) Content of Damage Assessments. At a minimum, damage assessments shall be in writing and contain the following:

"(1) Identification of the source, date, and circumstances of the compromise.

"(2) Classification of the specific information lost.

"(3) A description of the specific information lost.

"(4) An analysis and statement of the known or probable damage to the national security that has resulted or may result.

"(5) An assessment of the possible advantage to foreign powers resulting from the compromise.

"(6) An assessment of whether (i) the classification of the information involved should be continued without change; (ii) the specific information, or parts thereof, shall be modified to minimize or nullify the effects of the reported compromise and the classification retained; (iii) downgrading, declassification, or upgrading is warranted, and if so, confirmation of prompt notification to holders of any change.

"(7) An assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

"(8) An assessment of other appropriate corrective, administrative, disciplinary or legal actions.

"(c) System of Control of Damage Assessments. Each agency shall establish a system of control and internal procedures to ensure that damage assessments are performed in all cases described in paragraph (a), and that records are maintained in a manner that facilitates their retrieval and use within the agency.

"(d) Cases Involving More Than One Agency.

"(1) Whenever a compromise involves the classified information or interests of more than one agency, each department or agency undertaking a damage assessment shall advise other agencies of the circumstances and findings that affect their information or interests. Whenever a damage assessment, incorporating the product of two or more agencies is needed, the affected agencies shall agree upon the assignment of responsibility for the assessment.

"(2) Whenever a compromise occurs within an agency that is not responsible for the damage assessment, that agency shall provide all data pertinent to the compromise to the agency responsible for conducting the assessment.

"(3) Whenever a compromise of U.S. classified information is the result of actions taken by foreign nationals, by foreign government officials, or by U.S. nationals in the employ of international organizations, the agency performing the damage assessment shall ensure through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained. Whenever more than one agency is responsible for the assessment, those agencies shall coordinate the request prior to transmittal through appropriate channels.

"(4) Whenever an action is contemplated against any person believed responsible for the compromise of classified information, damage assessments shall be coordinated with appropriate agency legal counsel. Whenever a violation of criminal law appears to have occurred and a criminal prosecution is contemplated, the agency responsible for the damage assessment shall coordinate with the Department of Justice.

"(5) The designated representative of the Director of Central Intelligence, or other appropriate officials with responsibility for the information involved, will be consulted whenever a compromise of Sensitive Compartmented Information (SCI) has occurred."

EFFECTIVE: 03/15/94

26-13.2 Damage Assessment of Missing Files and Serials

A damage assessment must be conducted in accordance with MIOG, Part II, Section 26-13.1 for any classified file or serial missing for 30 days or more. This damage assessment must be reported as outlined in the Manual of Administrative Operations and Procedures, Part II, Section 2-4.3.8(1).

EFFECTIVE: 08/27/90

26-13.3 Cases Involving Loss or Unauthorized Disclosure of Sensitive Compartmented Information (SCI)

(1) The Director of Central Intelligence Directive (DCID) No. 1/19 sets forth the security policy for SCI. Compliance with this policy is mandatory for all Intelligence Community agencies that operate SCI programs.

(2) DCID No. 1/19 refers to the Senior Official of the Intelligence Community (SOIC) or his/her designee as the person responsible for ensuring DCID requirements are met. The SOIC has the responsibility for the granting, denial, and revocation of access to SCI.

(3) The Director, FBI, as the SOIC for the FBI, has delegated the authority to protect SCI to the Security Programs Manager (SPM), who is responsible for ensuring compliance with DCID requirements.

(4) Whenever there is a suspicion that there has been a serious compromise or unauthorized disclosure of SCI, an investigation will be conducted to determine if there is a reasonable likelihood that a compromise of SCI may have occurred, the identity of the person(s) responsible for the unauthorized disclosure, and the need for remedial procedures to preclude a recurrence. (See also 26-13.1.)

(5) If a compromise is determined to have occurred, the SPM will report the incident to the designated representative of the DCI. An investigation is to be conducted to identify full details of the violation/compromise, and to determine what specific information was involved, what damage resulted, and whether culpability was involved in the incident.

(6) If a case involves an inadvertent disclosure, the SPM

will exercise his/her judgment as to whether the interests of SCI security are served by seeking written agreements from unindoctrinated persons to whom SCI has been inadvertently disclosed. If the judgment is that those interests are so served, the person(s) involved signs the Inadvertent Disclosure Statement FD-722 (see 26-4.1), and the SPM has reason to believe that the person(s) will maintain absolute secrecy concerning the SCI involved, the report of investigation may conclude that no compromise occurred.

(7) Summaries of investigations and of related actions shall be provided to the DCI through the DCI's Unauthorized Disclosures Analysis Center by the SPM:

(a) when investigations show that the SCI was inadvertently disclosed to foreign nationals or deliberately disclosed to unauthorized persons; or

(b) when cases under investigation involve damage deemed significant by the SPM--espionage, flagrant dereliction of security duties, or serious inadequacy of security policies or procedures.

(8) The SPM will ensure that corrective action is taken in all cases of actual security violations and compromises.

EFFECTIVE: 08/27/90

26-14 CLEARANCES OF PERSONNEL HANDLING SENSITIVE COMPARTMENTED INFORMATION (SCI) MATERIAL

(1) All FBI employees requiring access to SCI material must be cleared prior to being granted access to that level of material. This includes couriers and individuals who type or otherwise process SCI material.

(2) All teletype operators, including alternates, must be cleared for access to "SI" material in order to facilitate round-the-clock transmission of "SI" information.

EFFECTIVE: 08/27/90

26-15 DESTRUCTION OF CLASSIFIED MATERIAL (See MIOG, Part II, 35-9.4.14.)

(1) When no longer needed, classified material shall be destroyed as soon as practicable by shredding, burning, pulverizing, pulping, melting, chemical decomposition, or other mutilation method sufficient to preclude any recognition or reconstruction of the information. (See MAOP, Part II, 2-1.3.)

(2) The destruction of Top Secret and Sensitive Compartmented Information (SCI) must be witnessed and recorded by two employees with security clearances commensurate with the classification of the material being destroyed. This information is to be recorded on the FD-501 and shall include the names of the employees, the reason for destruction, and the date, location and method of destruction.

EFFECTIVE: 07/26/95

SECTION 27. WITNESS SECURITY PROGRAM (WSP)

27-1 INTRODUCTION

[redacted]

b2
b7E

EFFECTIVE: 10/25/89

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

30 Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☑ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☑ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☑ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

_____ Page(s) withheld for the following reason(s): _____

☑ The following number is to be used for reference regarding these pages:
MIOG Pt II Sec 27 p1-31

XXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

EFFECTIVE: 05/13/96

SECTION 28. SEARCH AND SEIZURE OF DOCUMENTARY MATERIALS

28-1 ATTORNEY GENERAL'S GUIDELINES ON METHODS OF OBTAINING DOCUMENTARY MATERIALS HELD BY THIRD PARTIES

Pursuant to Title II, Privacy Protection Act of 1980 (Pub. L. 96-440, Sec. 201 et seq.; 42 U.S.C. 2000aa-11, et seq.), the Attorney General has issued the following guidelines in connection with the obtaining by Federal officers of documentary evidence in possession of third parties:

"Section 59.1 Introduction.

"(a) A search for documentary materials necessarily involves intrusions into personal privacy. First, the privacy of a person's home or office may be breached. Second, the execution of such a search may require examination of private papers within the scope of the search warrant, but not themselves subject to seizure. In addition, where such a search involves intrusions into professional, confidential relationships, the privacy interests of other persons are also implicated.

"(b) It is the responsibility of federal officers and employees to recognize the importance of these personal privacy interests, and to protect against unnecessary intrusions. Generally, when documentary materials are held by a disinterested third party, a subpoena, administrative summons, or governmental request will be an effective alternative to the use of a search warrant and will be considerably less intrusive. The purpose of the guidelines set forth in this part is to assure that federal officers and employees do not use search and seizure to obtain documentary materials in the possession of disinterested third parties unless reliance on alternative means would substantially jeopardize their availability (e.g., by creating a risk of destruction, etc.) or usefulness (e.g., by detrimentally delaying the investigation, destroying a chain of custody, etc.). Therefore, the guidelines in this part establish certain criteria and procedural requirements which must be met before a search warrant may be used to obtain documentary materials held by disinterested third parties. The guidelines in this part are not intended to inhibit the use of less intrusive means of obtaining documentary materials such as the use of a subpoena, summons, or formal or informal request.

"Section 59.2 Definitions.

"As used in this part ---

"(a) The term 'attorney for the government' shall have the same meaning as is given that term in Rule 54(c) of the Federal Rules of Criminal Procedure;

"(b) The term 'disinterested third party' means a person or organization not reasonably believed to be ---

"(1) A suspect in the criminal offense to which the materials sought under these guidelines relate; or

"(2) Related by blood or marriage to such a suspect;

"(c) The term 'documentary materials' means any materials upon which information is recorded, and includes, but is not limited to, written or printed materials, photographs, films or negatives, audio or video tapes, or materials upon which information is electronically or magnetically recorded, but does not include materials which constitute contraband, the fruits or instrumentalities of a crime, or things otherwise criminally possessed;

"(d) The term 'law enforcement officer' shall have the same meaning as the term 'federal law enforcement officer' as defined in Rule 41(h) of the Federal Rules of Criminal Procedure; and

"(e) The term 'supervisory official of the Department of Justice' means the supervising attorney for the section, office, or branch within the Department of Justice which is responsible for the investigation or prosecution of the offense at issue, or any of his superiors.

"Section 59.3 Applicability.

"(a) The guidelines set forth in this part apply, pursuant to section 201 of the Privacy Protection Act of 1980 (Sec. 201, Pub. L. 96-440, 94 Stat. 1879, (42 U.S.C. 2000aa-11)), to the procedures used by any federal officer or employee, in connection with the investigation or prosecution of a criminal offense, to obtain documentary materials in the private possession of a disinterested third party.

"(b) The guidelines set forth in this part do not apply to:

"(1) Audits, examinations, or regulatory, compliance,

or administrative inspections or searches pursuant to federal statute or the terms of a federal contract;

"(2) The conduct of foreign intelligence or counterintelligence activities by a government authority pursuant to otherwise applicable law;

"(3) The conduct, pursuant to otherwise applicable law, of searches and seizures at the borders of, or at international points of entry into, the United States in order to enforce the customs laws of the United States;

"(4) Governmental access to documentary materials for which valid consent has been obtained; or

"(5) Methods of obtaining documentary materials whose location is known but which have been abandoned or which cannot be obtained through subpoena or request because they are in the possession of a person whose identity is unknown and cannot with reasonable effort be ascertained.

"(c) The use of search and seizure to obtain documentary materials which are believed to be possessed for the purpose of disseminating to the public a book, newspaper, broadcast, or other form of public communication is subject to Title I of the Privacy Protection Act of 1980 (Sec. 101, et seq., Pub. L. 96-440, 94 Stat. 1879 (42 U.S.C. 2000aa, et seq.)), which strictly prohibits the use of search and seizure to obtain such materials except under specified circumstances.

"(d) These guidelines are not intended to supersede any other statutory, regulatory, or policy limitations on access to, or the use or disclosure of particular types of documentary materials, including, but not limited to, the provisions of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401, et seq.), the Drug Abuse Office and Treatment Act of 1972, as amended (21 U.S.C. 1101, et seq.), and the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970, as amended (42 U.S.C. 4541, et seq.).

"Section 59.4 Procedures.

"(a) Provisions governing the use of search warrants generally.

"(1) A search warrant should not be used to obtain documentary materials believed to be in the private possession of a disinterested third party unless it appears that the use of a subpoena,

summons, request, or other less intrusive alternative means of obtaining the materials would substantially jeopardize the availability or usefulness of the materials sought, and the application for the warrant has been authorized as provided in paragraph (a)(2) of this section.

"(2) No federal officer or employee shall apply for a warrant to search for and seize documentary materials believed to be in the private possession of a disinterested third party unless the application for the warrant has been authorized by an attorney for the government. Provided, however, that in an emergency situation in which the immediacy of the need to seize the materials does not permit an opportunity to secure the authorization of an attorney for the government, the application may be authorized by a supervisory law enforcement officer in the applicant's department or agency, if the appropriate United States Attorney (or where the case is not being handled by a United States Attorney's Office, the appropriate supervisory official of the Department of Justice) is notified of the authorization and the basis for justifying such authorization under this part within 24 hours of the authorization.

"(b) Provisions governing the use of search warrants which may intrude upon professional, confidential relationships.

"(1) A search warrant should not be used to obtain documentary materials believed to be in the private possession of a disinterested third party physician, lawyer, or clergyman, under circumstances in which the materials sought, or other materials likely to be reviewed during the execution of the warrant, contain confidential information on patients, clients, or parishioners which was furnished or developed for the purposes of professional counseling or treatment, unless ---

"(i) It appears that the use of a subpoena, summons, request or other less intrusive alternative means of obtaining the materials would substantially jeopardize the availability or usefulness of the materials sought;

"(ii) Access to the documentary materials appears to be of substantial importance to the investigation or prosecution for which they are sought; and

"(iii) The application for the warrant has been approved as provided in paragraph (b)(2) of this section.

"(2) No federal officer or employee shall apply for a warrant to search for and seize documentary materials believed to be

in the private possession of a disinterested third party physician, lawyer, or clergyman under the circumstances described in paragraph (b)(1) of this section, unless, upon the recommendation of the United States Attorney (or where a case is not being handled by a United Stares Attorney's Office, upon the recommendation of the appropriate supervisory official of the Department of Justice), an appropriate Deputy Assistant Attorney General has authorized the application for the warrant. Provided, however, that in an emergency situation in which the immediacy of the need to seize the materials does not permit an opportunity to secure the authorization of a Deputy Assistant Attorney General, the application may be authorized by the United States Attorney (or where the case is not being handled by a United States Attorney's Office, by the appropriate supervisory official of the Department of Justice) if an appropriate Deputy Assistant Attorney General is notified of the authorization and the basis for justifying such authorization under this part within 72 hours of the authorization.

"(3) Whenever possible, a request for authorization by an appropriate Deputy Assistant Attorney General of a search warrant application pursuant to paragraph (b)(2) of this section shall be made in writing and shall include:

"(i) The application for the warrant; and

"(ii) A brief description of the facts and circumstances advanced as the basis for recommending authorization of the application under this part.

"If a request for authorization of the application is made orally or if, in an emergency situation, the application is authorized by the United States Attorney or a supervisory official of the Department of Justice as provided in paragraph (b)(2) of this section, a written record of the request including the materials specified in paragraphs (b)(3)(i) and (ii) of this section shall be transmitted to an appropriate Deputy Assistant Attorney General within 7 days. The Deputy Assistant Attorneys General shall keep a record of the disposition of all requests for authorizations of search warrant applications made under paragraph (b) of this section.

"(4) A search warrant authorized under paragraph (b)(2) of this section shall be executed in such a manner as to minimize, to the greatest extent practicable, scrutiny of confidential materials.

"(5) Although it is impossible to define the full range of additional doctor-like therapeutic relationships which involve the furnishing or development of private information, the United States

Attorney (or where a case is not being handled by a United States Attorney's Office, the appropriate supervisory official of the Department of Justice) should determine whether a search for documentary materials held by other disinterested third party professionals involved in such relationships (e.g., psychologists or psychiatric social workers or nurses) would implicate the special privacy concerns which are a dressed in paragraph (b) of this section. If the United States Attorney (or other supervisory official of the Department of Justice) determines that such a search would require review of extremely confidential information furnished or developed for the purposes of professional counseling or treatment, the provisions of this subsection should be applied. Otherwise, at a minimum, the requirements of paragraph (a) of this section must be met.

"(c) Considerations bearing on choice of methods.

"In determining whether, as an alternative to the use of a search warrant, the use of a subpoena or other less intrusive means of obtaining documentary materials would substantially jeopardize the availability or usefulness of the materials sought, the following factors, among others, should be considered:

"(1) Whether it appears that the use of a subpoena or other alternative which gives advance notice of the government's interest in obtaining the materials would be likely to result in the destruction, alteration, concealment, or transfer of the materials sought; considerations, among others, bearing on this issue may include:

"(i) Whether a suspect has access to the materials sought;

"(ii) Whether there is a close relationship of friendship, loyalty, or sympathy between the possessor of the materials and a suspect;

"(iii) Whether the possessor of the materials is under the domination or control of a suspect;

"(iv) Whether the possessor of the materials has an interest in preventing the disclosure of the materials to the government;

"(v) Whether the possessor's willingness to comply with a subpoena or request by the government would be likely to subject him to intimidation or threats of reprisal;

"(vi) Whether the possessor of the materials has

previously acted to obstruct a criminal investigation or judicial proceeding or refused to comply with or acted in defiance of court orders; or

"(vii) Whether the possessor has expressed an intent to destroy, conceal, alter, or transfer the materials;

"(2) The immediacy of the government's need to obtain the materials; considerations, among others, bearing of this issue may include:

"(i) Whether the immediate seizure of the materials is necessary to prevent injury to persons or property;

"(ii) Whether the prompt seizure of the materials is necessary to preserve their evidentiary value;

"(iii) Whether delay in obtaining the materials would significantly jeopardize an ongoing investigation or prosecution; or

"(iv) Whether a legally enforceable form of process, other than a search warrant, is reasonably available as a means of obtaining the materials. The fact that the disinterested third party possessing the materials may have grounds to challenge a subpoena or other legal process is not in itself a legitimate basis for the use of a search warrant.

"Section 59.5 Functions and Authorities of the Deputy Assistant Attorneys General.

"The functions and authorities of the Deputy Assistant Attorneys General set out in this part may at any time be exercised by an Assistant Attorney General, the Associate Attorney General, the Deputy Attorney General, or the Attorney General.

"Section 59.6 Sanctions.

"(a) Any federal officer or employee violating the guidelines set forth in this part shall be subject to appropriate disciplinary action by the agency or department by which he is employed.

"(b) Pursuant to section 202 of the Privacy Protection Act of 1980 (Sec. 202, Pub. L. 96-440, 94 Stat. 1879 (42 U.S.C. 2000aa-12)), an issue relating to the compliance, or the failure to comply, with the guidelines set forth in this part may not be litigated, and a court may not entertain such an issue as the basis for the suppression or exclusion

of evidence."

EFFECTIVE: 02/23/84

SECTION 29. TERRORIST RESEARCH AND ANALYTICAL CENTER (TRAC)

29-1 DEFINITION

The TRAC is responsible for conducting research on terrorism, analyzing the data received, and making assessments of the potential terrorist threats to the United States.

EFFECTIVE: 02/23/84

29-2 SERVICES

(1) To computerize data on all domestic and international terrorist groups which pose a threat to the United States.

(2) To conduct research on terrorist groups, analyze data, and produce assessments of the potential dangers posed by those groups to the United States.

(3) To record, maintain, analyze, and publish statistical information concerning terrorism and terrorist incidents in the United States and the accomplishments of the FBI's counterterrorism efforts.

(4) To prepare the terrorism program budget submissions.

(5) To maintain a terrorist reference library consisting of books, periodicals, newspapers, NEXIS (a computer assisted public information source), slides and audio video cassettes on various terrorist-related incidents, and a vertical file which contains indexed research material consisting of papers produced by TRAC personnel and papers which are primary and secondary sources of information in research as well as papers ephemeral in nature usually of temporary interest.

(6) To administer a terrorism training program.

EFFECTIVE: 02/23/84

SECTION 30. |CRISIS MANAGEMENT PROGRAM|

30-1 CRISIS MANAGEMENT PROGRAM| (See MIOG, Part I, 261-2(6), NFIP Manual, Part I, 8-1.1.)|

(1) Crisis management is the process of identifying, acquiring, and planning the use of resources needed to anticipate, prevent, and/or resolve a crisis. The program, as it currently exists in the Bureau, encompasses two other major programs: crisis (hostage) negotiation and special weapons and tactics (SWAT). However, these are not the only resources involved in crisis management.

(2) The components (resources) that may be included on any crisis management team are:

(a) Managerial

(b) Negotiators

(c) Tactical (SWAT/Hostage Rescue Team (HRT))

(d) Technical

(e) Investigative

(f) Support

(g) Special Operations Groups (SOG)

(h) Legal

(i) Media Representative

(3) Crisis management involves planning the use of these components and coordinating their actions at the crisis scene.

EFFECTIVE: 02/27/96

30-1.1 Objectives

(1) To preserve life.

(2) To enforce the laws over which the FBI has jurisdiction.

In keeping with these objectives, the guiding principle in negotiation/SWAT employment, as in all actions in a given crisis, should be to minimize the risks to all persons involved: hostages, bystanders, subjects, and law enforcement officers.

EFFECTIVE: 01/18/91

30-1.2 Control of a Crisis Management Team (CMT)

(1) Operational and administrative control of crisis management components lies with the SAC within the respective field office, except in certain unusual or major cases such as those involving dignitaries, diplomats, a large hostage population, or cases involving national or international impact, in which direct operational control may be assumed by the Assistant Director (AD), Criminal Investigative Division (CID), or AD, Intelligence Division (INTD), FBIHQ, or their designated representative. The SAC of the office employing crisis management components must personally assume direct management responsibility and control of those components.

(2) The SAC or his/her designated representative must assume the responsibility of on-scene commander (OSC) during a crisis incident. It is the duty of the SAC/OSC to determine the overall strategy for responding to and/or resolving a crisis incident. The crisis management component leaders will then devise specific tactics/procedures to support the SAC/OSC's strategy. These tactics/procedures are all subject to the approval of the SAC/OSC.

(3) The Crisis Management, Negotiation, and SWAT Programs are coordinated at the FBIHQ level by a program manager working in the Special Operations and Research Unit (SOARU) in the Training Division. Training Division, through the SOARU, is responsible for crisis management, negotiation, and SWAT training; doctrinal development; research and evaluation; advisory services; certain logistic support to the field; and operational support to FBIHQ and the field.

EFFECTIVE: 01/18/91

30-1.3 Crisis Management Plans

(1) The preparation of plans to anticipate and respond to specific crisis situations is imperative.

(2) The following procedures should be used when preparing such plans:

(a) Identify potential crisis situations.

(b) Prioritize potential crisis situations.

(c) Determine what is expected of the Bureau during the crisis (objectives).

(d) Make provisions to acquire the resources needed to accomplish your objectives.

(e) Identify sources of intelligence:

1. Human--collect background/descriptive information on subjects, employees, occupants, and others having access to crisis site.

2. Physical--conduct a thorough site survey of the crisis site.

(f) Develop strategies and tactics--developing the overall strategy for a particular crisis situation is a command function. Once the strategy is determined, the other components of the CMT develop specific tactics to support the overall strategy of the OSC.

(g) Determine command/control/communications requirements.

1. If it is a joint operation, determine who will be the lead agency. Once this is decided, designate a chain of command.

2. Select location for a command post.

3. Design a communications format.

(h) Determine logistics required to support the overall response to the crisis.

(i) Establish liaison and coordination with contributing agencies and services.

(j) Commit plan to paper.

(k) Test the plan and modify accordingly.

(l) Disseminate the plan to appropriate personnel.

EFFECTIVE: 01/18/91

30-1.4 Decision Making

Decisions must be made while working within the context of the crisis management plan to assure an acceptable solution. When in a decision-making mode, it is helpful to include others in the decision-making process and weigh decisions against preestablished criteria.

(1) Action criteria should consider:

(a) Necessity--is the contemplated action necessary at this time within the context of the crisis event?

(b) Risk effectiveness--is the contemplated action warranted because it will reduce risk? Or will it increase risk?

(c) Acceptability--is the contemplated action legally and ethically acceptable?

(2) Having clearly defined objectives when planning for a particular crisis (and being able to prioritize them) will facilitate good decision making.

EFFECTIVE: 01/18/91

30-1.5 Command Post (CP) Procedures

(1) Some type of CP is necessary to coordinate the actions of multiple units, especially when they are engaged in multiple activities, or when the number of individuals involved in a crisis situation exceeds the span of control of the OSC.

(2) Prior to setting up the CP, the following steps should be taken:

(a) Establish a command structure to include all crisis management components being used. This chain of command must be communicated and formally posted.

(b) Assign responsibilities to the components of the command structure (mission).

(c) The leader of each component must be delegated the authority to successfully accomplish that component's mission.

(d) Design an organizational format for the CP.

(e) Develop a standing operating procedure (SOP) for the CP. This SOP should outline a procedure for the gathering and processing of intelligence. All components represented in the CP must have a system that enables them to receive, analyze, file, and retrieve intelligence. The SOP should also outline procedures for communicating this intelligence to the on-scene commander and other components in the CP.

(f) When possible, use an advisory staff in the CP. The SAC will designate an individual to act as a representative of each component of the CMT. This individual should preferably be a supervisor who is familiar with the capabilities and limitations of that particular component. This group of supervisors/Special Agents will be called advisors (e.g., SWAT advisor, negotiation advisor) and will form the SAC's advisory staff. In crisis situations where the SAC and his/her CP are in close proximity to the actual component leaders, the use of an advisory staff would not be absolutely necessary. However, in crisis situations where the SAC and his/her CP are not in close proximity to the component leaders, there are certain advantages to using the advisory staff:

1. It enables the component leader to be with, and function with, his/her team, which is the best place for the team leader to be.

2. It provides the SAC with a knowledgeable staff that is always in the CP and prepared to answer any questions regarding a particular component.

3. It provides the SAC with an individual in the CP that will receive, analyze, file, and retrieve intelligence from a particular component.

(g) In addition to an advisor for each component of the CMT, the SAC will also designate a crisis management advisor in the CP. This individual will ensure the CP is operating in accordance with the SAC's CP procedures. The crisis management advisor can identify problem areas and correct them before any serious problems occur. This advisor will also ensure all components are communicating and coordinating all their actions at the crisis site.

EFFECTIVE: 01/18/91

30-1.6 Field Office Response to Crisis Situations (See MIOG, Part I, 252-1.7.)

(1) The crisis management assets of most field offices may not be capable of adequately handling a major or protracted crisis situation without additional assets. When it becomes apparent a crisis situation will continue for more than 24 hours, the SAC may contact surrounding field offices for additional resources.

(2) The SOARU has divided the 56 field offices into eight districts and 16 regions. Each district contains one to three regions, and each region contains from two to five field offices. Any field office that is faced with a crisis situation demanding a response exceeding its capability can call upon its region for additional resources. The districts and regions are structured as follows: (See 30-2.2(2) and 30-3.2(3).)

FIELD SWAT DISTRICT/REGION ASSIGNMENTS

DISTRICT 1

Region 1	Region 2	Region 3
[redacted]	[redacted]	[redacted]

b2
b7E

[redacted]

DISTRICT 2

Region 4 [redacted]

Region 5 [redacted]

Region 6 [redacted]

DISTRICT 3

Region 7 [redacted]

DISTRICT 4

b2
b7E

Region 9 [redacted]

Region 10 [redacted]

Region 11 [redacted]

DISTRICT 5

DISTRICT 6

Region 8 [redacted]

Region 12 [redacted]

Region 13 [redacted]

DISTRICT 7

DISTRICT 8

Region 14 [redacted]

Region 15 [redacted]

Region 16 [redacted]

[redacted] [redacted]

b2
b7E

* Denotes the [redacted] Enhanced District Teams
( ) Denotes SWAT Complement w/56 Field Offices TOTAL [redacted]

(3) In confrontations necessitating employment of force involving an extraordinary degree of risk and which, in the judgment of the SAC, exceed FBI SWAT capability, the AD, CID, or AD, National Security Division, or their representative, should be advised in the event specialized tactical intervention may be requested. The FBI entity charged with responding to these incidents is the HRT. The HRT may be requested through CID, Violent Crimes and Major Offenders Section, FBIHQ.

EFFECTIVE: 08/29/94

30-1.7 Training

(1) At Quantico:

(a) Four days of crisis management training is conducted during Executive Development Institute (EDI) training sessions.

(b) One day of crisis management training is conducted during FBI Supervisors' Management Seminars.

(2) In the field:

(a) Each field office must conduct at least one training session per year that enables the components of the crisis management team to interact in a realistic crisis scenario. This training session should include a command post exercise (CPX) and field training exercise (FTX).

(b) The SAC and his/her management staff must be directly involved in this training session.

(c) The negotiation and SWAT components are mandated to participate in one regional training session each year. The host field office of the regional training session should conduct their

crisis management training during this regional training session (see (a) above).

(d) Training Division recommends that all crisis management components interact and train together whenever possible.

EFFECTIVE: 01/18/91

30-1.8 Reporting Procedures

(1) Each field office will submit semiannual reports on the utilization of their crisis management components, furnishing the following data:

(a) Date of use.

(b) Bureau and field office file number, title, and character of case.

(c) A brief account of the activity, specifically outlining the role played by each component of the CMT.

(d) The negotiation and SWAT components will also include enclosures to this report, detailing specific information regarding these components. Specifics are enumerated in the Crisis Negotiation and SWAT Program sections that follow.

(2) Reports are due by the 15th day of April and October, for the previous six months. They must be transmitted by cover airtel to the Director, FBI, Attention: Training Division, Special Operations and Research Unit.

EFFECTIVE: 01/18/91

30-2 CRISIS (HOSTAGE) NEGOTIATION PROGRAM

(1) Crisis negotiation is the process of using specific techniques (relying heavily on verbal communications) to bring about a desired behavioral change on the part of an individual who may pose a threat to himself/herself or others, and to offer an alternative to (or support of) tactical intervention in raids, arrests, and rescues.

(2) Specially trained and equipped Agent volunteers will function as part of a field office crisis management team. This crisis negotiation team can greatly reduce the risks associated with handling hostage, kidnap, barricade, and/or suicide situations and increase the options available to the SAC in dealing with such events.

EFFECTIVE: 01/18/91

30-2.1 Control of Negotiators

(1) Operational and administrative control of negotiators is the same as mentioned in 30-1.2(1).

(2) The SOARU also manages the FBI's Critical Incident Negotiation Team (CINT). The CINT is comprised of the FBI's most experienced negotiators who have a specialized investigative and/or foreign language capability. CINT members are afforded advanced training in negotiation and terrorism to include nuclear, chemical, and biological negotiation considerations. This team is considered a national resource for the FBI and is deployed at the direction of FBIHQ through contact with the SOARU.

EFFECTIVE: 01/18/91

30-2.2 Organization

(1) Each field office will have a crisis negotiation team with a minimum of three trained negotiators. The eight field offices that have the enhanced SWAT district teams will have a minimum of six trained negotiators. Larger field offices or offices with distant resident agencies should have additional Agents trained as negotiators. The total number of negotiators in a field office should be based on the geographical area covered, the population density, and the potential for utilization.

(2) Any field office facing an event demanding a response exceeding its capability can call upon its region for negotiator support. The districts and regions are structured as indicated in the district chart at 30-1.6(2).

(3) The configuration of the negotiation team within each field office is left to the discretion of the SAC, but it must always have two negotiators per shift--a primary and a secondary negotiator. This team may be supported by additional negotiators as needed.

(4) SACs will appoint a negotiation coordinator charged with the responsibility of being familiar with team capability. The negotiation coordinator should be an individual who has served satisfactorily as a team member and has a good working knowledge of basic negotiation and tactical concepts.

(5) The negotiation coordinator should act as negotiation advisor and representative in the CP during operations.

EFFECTIVE: 01/18/91

30-2.3 Utilization

Negotiators will deploy with the field office SWAT team in any situation posing a higher-than-normal risk factor in which the SWAT team could anticipate encountering a potential barricade, suicide, or hostage situation. Such deployments should be based on available intelligence concerning the subject, weapons, and location.

EFFECTIVE: 01/18/91

30-2.4 Qualifications for Negotiation Team Members

(1) Agents assigned to negotiation teams in the field must have satisfactorily completed the two-week basic negotiation training course at the FBI Academy.

(2) Negotiation candidates should be:

(a) Volunteers.

(b) In excellent physical condition.

(c) Emotionally capable of functioning in a prolonged high-stress situation.

(d) An FBI Agent for at least three years.

Experience as a police officer, military service, or having a behavioral science background is also desirable and could be considered an exception to item (2)(d) above.

EFFECTIVE: 01/18/91

30-2.5 Reporting

As set forth in 30-1.8(1)(a)-(c), each field office is required to submit semiannual crisis management reports. The following additional negotiation data is to be furnished as an enclosure in this designated format:

I. New tactics, techniques, concepts of operations or equipment successfully employed in negotiation operations during the reporting period.

II. Problems encountered relative to negotiation operation during the reporting period.

III. Team status:

A. Specialized training needed by your office.

B. Official Bureau name of each team member.

C. The identity of the negotiation coordinator.

D. Number of days devoted to team training this reporting period.

EFFECTIVE: 01/18/91

30-2.6 Training

(1) At Quantico:

(a) Basic negotiation training will consist of a two week course at the FBI Academy.

(b) Specialized regional training courses will be held every year as required.

(2) In the field:

(a) Training will consist of a minimum of six days per year. The maximum is to be determined by the SAC and his/her special needs.

(b) Each field office negotiation team will participate in one regional training session per year where the host office conducts a CPX/FTX. The negotiation team will also participate in the one mandatory crisis management training session per year in their respective field office.

(c) The SAC must personally participate when his/her office is hosting a regional training session. This responsibility is not to be delegated.

EFFECTIVE: 01/18/91

30-2.7 Management of Negotiation Teams

(1) To fully utilize the capabilities of the negotiation team, the command of the team must be delegated to the negotiation coordinator by virtue of his/her training with the team and familiarity with the capabilities of the team.

(2) The SAC or his/her designated representative must assume the responsibility of OSC during a crisis incident. It is the duty of the SAC/OSC to determine the overall strategy for responding to and/or resolving a crisis incident. The negotiation coordinator will then devise specific negotiation tactics/procedures to support the SAC/OSC's strategy. These negotiation tactics/procedures are all subject to the approval of the SAC/OSC.

(3) Negotiation team deployment on a regional or district

basis, or when the HRT is operationally deployed, will be supported by the SAC from the host office, or his/her ASAC in the event he/she is not available. The SAC/OSC will promptly designate a senior negotiation coordinator as the overall negotiation commander and ensure that the chain of command is understood by all personnel present.

EFFECTIVE: 01/18/91

30-2.8 Joint Operations

(1) Many FBI operations involve close work with other law enforcement agencies, and this relationship may necessarily extend to hostage or barricade situations involving FBI and police negotiation teams.

(2) Due to the wide divergence of training, procedures, and professional competency of police negotiation teams, the integration of police and FBI negotiation teams in a given operation should be approached with caution from standpoints of effectiveness, safety, and legal liability.

(3) In joint operations, it is imperative that unified negotiation teams be established at the outset with one person clearly in charge of all negotiations, preferably the most experienced FBI negotiation team leader present. The arbitrary assumption of command by the FBI, particularly if police units are first on the scene, as they frequently are, could be a sensitive and provocative maneuver requiring tact and diplomacy on the parts of the SAC and negotiation coordinator.

(4) The decision to engage in a joint operation must be made by the SAC and should be based on the recommendations of the negotiation coordinator, his/her team, and all other factors bearing on mission safety and effectiveness.

EFFECTIVE: 01/18/91

30-2.9 Use of FBI Negotiators in Non-FBI Matters

(1) |Office of the General Counsel (OGC)|has reviewed the use of FBI Special Agent negotiators in non-Federal matters. |OGC| opined that FBI negotiators could actively participate in situations lacking clear Federal jurisdiction where the Special Agent negotiator is either the first person on the scene or where there is no state or local negotiator available.

(2) |OGC|further advised hostage situations, by their very nature, involve emergency circumstances that would justify an FBI response even where a Federal violation is not readily apparent. Even if an FBI negotiator was not actually doing the negotiating, the FBI negotiator could still furnish advice or consultation on the scene as part of our training responsibilities under Title 28, Code of Federal Regulations, Section 0.85(e).

(3) Title 42, USC, Section 3774(a) authorizes the Director of the FBI to assist in conducting training of state or local law enforcement entities and conveys some Federal authority on which FBI negotiators can operate in non-Federal situations.

(4) Two guidelines concerning the role of an FBI negotiator providing assistance to local authorities in a non-Federal offense must be adhered to:

(a) The FBI negotiator must remain under the control of his/her SAC as opposed to the local authorities.

(b) FBI negotiators should be extricated from the actual negotiations, using their best professional judgment, once trained local officers arrive and are in a position to safely assume responsibility for the situation.

EFFECTIVE: 09/09/94

30-3 SPECIAL WEAPONS AND TACTICS (SWAT) PROGRAM

The SWAT Program is a concept based on the premise that a select group of highly motivated and well-conditioned Agent volunteers, specially equipped and trained to function as a team, can greatly reduce the risks associated with handling unusually dangerous raids, arrests, and rescues, and increase the options available to the SAC in dealing with such events.

EFFECTIVE: 01/18/91

30-3.1 Control of SWAT

Operational and administrative control of SWAT is the same as mentioned in 30-1.2(1).

EFFECTIVE: 01/18/91

30-3.2 Organization

(1) Each FBI field office has a primary SWAT unit, the size of which varies from office to office, depending upon geographical area covered, population density, and the potential for violent crime within FBI jurisdiction. Additionally, the eight technically enhanced district teams are configured to provide technical and operational support to field offices within their geographic districts.

(2) The size of office primary units may be increased only by FBIHQ, based upon recommendations of the SAC, supported by well documented rationale. Additional requests for manpower increases will not be approved by FBIHQ without identifying corresponding reductions elsewhere.

(3) Realizing that the relatively small teams in most offices will not be sufficient to handle major or protracted problems, the field has been divided into eight districts and 16 regions. Each district contains one to three regions and each region contains from two to five offices. Any office facing an event demanding a response exceeding its capability can call upon its region

for reinforcement, not only for SWAT personnel, but other crisis management assets. Should an event exceed the capability of any specific region or require specialized equipment not in the possession of that field office, an SAC may request assistance from his/her district team. Requests for regional or district support, however, should be kept to a minimum. When requested, this support may be for equipment only, equipment and a minimum number of operators, or more extensive reinforcement. The districts and regions are structured as indicated in the district chart in 30-1.6(2), with the primary SWAT complement designated in parentheses.

(4) Primary team members will be supported with training and equipment by the Training Division. Each SAC is authorized to develop and maintain reserve teams as needed, but they must be supported by utilizing field resources. Reserve teams will participate in monthly field SWAT training at the discretion of the SAC.

(5) The configuration of teams within each office is left to the discretion of the SAC, except that all primary team members should be assigned to headquarters city.

(6) Each primary team within an office must be directed by a team leader selected by the SAC from the primary members. If an office has more than one team, a senior team leader must be appointed among the primary team leaders to manage all SWAT teams within the office.

(7) SACs will appoint a separate SWAT advisor, preferably a Supervisory Special Agent charged with the responsibility of being familiar with team capability and acting in the capacity of tactical advisor and SWAT representative in the command post during operations.

(8) The SWAT advisor should be an individual who has previously served satisfactorily as a team member and has a good working knowledge of basic tactical concepts but is no longer a participant on a team.

EFFECTIVE: 01/18/91

||30-3.3| Utilization

(1) A raid, arrest or other situation posing a higher-than-normal risk factor will necessitate the use of a SWAT unit for planning and execution whenever practicable to reduce the risk to Agents, innocent persons, and subjects.

(2) The determination as to whether a given situation meets "higher-than-normal risk" criteria will be made by the SAC or ASAC based upon assessment of the following factors:

(a) Subjects--number, motivation, training, propensity to violence, and other indicators.

(b) Hostages (if any)--number, location, medical histories, etc.

(c) Objective (crisis point)--location, defensibility, size configuration, avenues of approach, etc.

(d) Weapons--types, numbers, lethality.

(3) It is not the intent of this policy to place all raids and arrests in the hands of SWAT teams, but rather to reduce the risks to all personnel involved in those relatively few situations which would pose unwarranted danger if handled by traditional means.

EFFECTIVE: 01/18/91

||30-3.4| Qualifications for SWAT Team Members

(1) Agents assigned to primary SWAT teams in the |field|must|have satisfactorily completed basic SWAT training at the FBI Academy; however, an Agent who has not met this requirement may be assigned to a primary team provided (a) he/she receives as much basic training in the field as possible and (b) that he/she satisfactorily completes basic SWAT training at the FBI|Academy, or the FBIHQ-authorized field equivalent using the SWAT lesson plans at monthly training sessions, |as soon as possible following his/her placement on a primary team.

(2) Candidates for SWAT duty should be:

(a) Volunteers.

(b) In excellent physical condition.

(c) Emotionally stable.

(d) Proficient and confident in the use of small firearms.

Experience as a police officer, military combatant, firearms, and/or defensive tactics instructor is also desirable.

(3) It is desirable, but not mandatory, that reserve SWAT teams consist of Agents who have completed basic SWAT training.

(4) It is also desirable, but not mandatory, that candidates have at least three years of experience in the field.

EFFECTIVE: 01/18/91

30-3.5 Reporting

As set forth in 30-1.8(1)(a)-(c), each field office is required to submit semiannual crisis management reports. The following additional SWAT data is to be furnished as an enclosure in this designated format:

I. New tactics, techniques, concepts of operation or equipment successfully employed in SWAT operations during the reporting period should be set forth.

II. Problems encountered relative to SWAT operation during the reporting period should be included in the report.

III. Team status to include authorized SWAT complement.

A. Specialized training needed by your office.

B. Official name of each primary team member.

C. Identity of senior team leader (and subordinate team leaders if more than one team).

D. The identity of SWAT advisor.

E. The identities of primary team members who have not completed basic SWAT training.

F. Number of days and hours devoted to team training this reporting period, broken down by tactical subject.

Semiannual reports should include an FD-39, reporting firearms qualification scores.

EFFECTIVE: 01/18/91

30-3.6 Training

(1) At Quantico:

(a) Basic SWAT training will consist of a two-week course at the FBI Academy.

(b) Specialized in-service courses will be held every two to three years or as required.

(c) Only primary team members will be eligible for SWAT training at the FBI Academy.

(2) In the field:

(a) Training will consist of a minimum of the equivalent of one day per month, except district teams which are mandated to conduct a minimum of two days of training each month. The maximum is to be determined by the SAC and his/her special needs, but this training is not to exceed five days per month. Any request in addition to the five days per month must be fully justified and approved by SOARU, Training Division, FBIHQ.

(b) Each field office SWAT team will participate in one regional training session per year where the host office conducts a CPX/FTX. The SWAT team will also participate in the one mandatory crisis management training session per year in their respective field office.

(c) The SAC must personally participate when his/her office is hosting a regional training session. This responsibility is not to be delegated.

EFFECTIVE: 01/18/91

||30-3.7| Management of SWAT Teams

(1) To fully utilize the effectiveness and capability of SWAT teams, the direct tactical command of the units must be delegated to the team leader by virtue of his/her training with the team and his/her familiarity with its capabilities. This in no way alters the overall command responsibility and authority of the SAC within his/her field|office.|

(2) |The SAC or his/her designated representative must assume the responsibility of OSC during a crisis incident. It is the duty of the SAC/OSC to determine the overall strategy for responding to and/or resolving a crisis incident. The SWAT team leader will then devise specific tactics/procedures to support the SAC/OSC's strategy. These tactics/procedures are all subject to the approval of the SAC/OSC, with the exception of emergency self-defense measures and immediate-response deployment. It is the responsibility of the SWAT team leader to personally direct the team in the execution of an approved plan.|

|(3)| Time and circumstances permitting, an inspection of personnel and a rehearsal of the tactical plan should be conducted before the plan is executed.

|(4)| SWAT team deployment on a regional|or district basis, or when the HRT is operationally deployed, will|be supported by the SAC from the host|office,|or his/her ASAC in the event he/she is not available. This individual|will|promptly designate a senior SWAT leader as the overall tactical commander and ensure that the chain of command is understood by all personnel present.

EFFECTIVE: 01/18/91

30-3.8 Fire Discipline

(1) Any confrontation should be managed with minimal use of weapons fire.

(2) Much emphasis is placed on fire discipline during initial SWAT training and must continue in field training. Personnel on the scene of a confrontation who have not had SWAT training must be thoroughly briefed by the senior SWAT team leader concerning use of firearms in the context of problem solution.

(3) Use of deadly force by SWAT personnel is governed by the same policy applicable to all Special Agents. (See MIOG, Part II, 12-2.1.)

(4) Meeting the above criteria, however, does not justify indiscriminate "area" type firing. All use of firepower must be preceded by acquisition of a known hostile target. This does not preclude the directing of selective suppressive fire at a low visibility target (such as a window from which gunfire is emanating) to cover movement of personnel, rescue of wounded individuals or evacuation of innocents.

(5) The use of shotgun breaching as a forced entry technique is authorized for all SWAT teams. (However, appropriate training is required as set forth in MAOP, Part II, 8-9.) It can be deployed concurrent with SAC approval, consistent with FBI deadly force guidelines, using only Bureau-approved frangible shotgun rounds. Using frangible rounds does not create unreasonable risks; those risks that may exist can be mitigated by ensuring that in each case where the use of this technique is contemplated, the following factors are carefully weighed:

(a) The presence and number of individuals inside the building to be breached;

(b) Proximity of those individuals to the area to be breached;

(c) Whether innocent persons are at risk; and

(d) The risk of primary or secondary fragmentation. See MAOP, Part II, 8-9.3(4).

(6) Likewise, the use of chemical agents must be extremely judicious, with a minimum number of grenades injected to

dislodge subject(s). Use of chemical agents also necessitates standby fire-fighting equipment. Explosive ordnance disposal technicians may be required to remove dud 40 mm munitions. (See MIOG, Part II, 12-14.1 and 12-14.2 for chemical agent policy and procedures.)

EFFECTIVE: 04/07/97

30-3.9 Joint Operations

(1) Many FBI operations involve close work with other law enforcement agencies; and from a realistic viewpoint, it is realized that this relationship may necessarily extend to raid and arrest situations involving FBI and police tactical units.

(2) Due to the wide divergence of training, procedures, and professional competency of police SWAT units, the integration of police and FBI teams in a given operation should be approached with caution from standpoints of effectiveness, safety, and legal liability. If necessary to combine units, teams should remain intact and be separated by function. For instance, in a raid requiring joint operations, police SWAT units might be assigned the cover function and FBI teams the apprehension function. But under no circumstances should personnel from police SWAT units be integrated into FBI teams or vice versa.

(3) In joint operations, it is imperative that unified tactical command be established at the outset with one person clearly in charge of all operations within the inner perimeter, preferably the most experienced FBI SWAT leader present. Briefing in preparation for joint operations should follow the "operations order" format as set out in Training Division handouts.

(4) It is realized that arbitrary assumption of command by the FBI, particularly if police units are first on the scene as they frequently are, could be a sensitive and provocative maneuver requiring tact and diplomacy on the parts of the SAC and senior SWAT team leader.

(5) The decision to engage in a joint operation must be made by the SAC and should be based on recommendations of the senior team leader, his/her unit, and all other factors bearing on mission safety and effectiveness.

|(6)| In confrontations necessitating employment of force involving an extraordinary degree of risk and which, in the judgment of the SAC, exceed FBI|SWAT|capability, the AD, CID, or AD, INTD, FBIHQ, or their representative should be advised in the event specialized|HRT|intervention may be requested.

EFFECTIVE: 01/18/91

||30-3.10| Weapons

Certain weapons in the FBI arsenal were acquired specifically for SWAT applications and should be assigned to team members for their exclusive use. They are:

[redacted]

b2
b7E

FBI firearms instructors may utilize these weapons when instructing SWAT personnel.

EFFECTIVE: 01/18/91

|SECTION 31. DEPUTATION PROGRAM

31-1 BACKGROUND

(1) Historically, the Attorney General has had the authority to supervise and direct the United States Marshals Service (USMS) in the performance of public duties. Specifically, the Attorney General is empowered to authorize the appointment of Special Deputy U.S. Marshals. In June 1984, this authority was delegated to the Associate Attorney General. The Associate Attorney General exercised his authority to direct the USMS to deputize state and local law enforcement officers to enable those officers to handle federal law enforcement functions while under the supervision of the FBI. Neither the FBI nor the Drug Enforcement Administration had independent deputation authority.

(2) Effective 10/27/86, Title 21, United States Code, Section 878 was amended by the enactment of the Anti-Drug Abuse Act of 1986. This legislation added state and local law enforcement officers to those who may be deputized by the Attorney General to carry firearms, execute warrants, serve subpoenas, make arrests and seizures, and carry out other federal drug law enforcement duties as determined by the Attorney General. The Attorney General no longer had to rely on the USMS to deputize officers assisting|the FBI in|drug investigations. In fact, the USMS|had|taken the position that it does not have the authority to make drug-related deputations. The Attorney General has delegated this deputation authority to the Director and on 8/4/87, the FBI assumed responsibility for deputizing officers assisting in FBI drug investigations. |On 3/24/95, the Director delegated Title 21 deputation authority to Special Agents in Charge (SAC).| An FBI-deputized officer is referred to as a Special Federal|Officer (SFO).| The Deputation Program is managed by the |Administrative Unit, Operational|Support Section, Criminal Investigative Division (CID).

EFFECTIVE: 08/09/95

31-2 SCOPE OF DEPUTATION AUTHORITY

(1) Special Federal Officers are authorized to investigate, under FBI supervision, violations of Title 21 and those drug-related violations falling within the FBI's jurisdiction that arise out of an investigation predicated on drug violations.

(2) The scope of this authority is limited to those violations that are so inextricably linked to the Title 21 predicate that it could be fairly said that they would not have been engaged in separate and apart from the drug violations.

(a) For example, if during a drug investigation it was established that the subjects were engaged in money laundering, it would be reasonable to conclude that the subjects would not have engaged in this activity absent their primary involvement in drug trafficking. On the other hand, if during a drug investigation it was determined that the subjects were engaged in criminal activity totally unrelated to their drug trafficking, it would not be reasonable to conclude that there was a connection between the two violations.

(b) The fact that a nondrug violation is developed during a drug investigation is insufficient to empower a Special Federal Officer to investigate the violation if it did not arise out of the Title 21 predicate offense.

(c) Special Federal Officers do not possess general authority to act as FBI Special Agents.

(3) The USMS remains responsible for deputizing officers participating in FBI investigations which do not fall within the scope of the FBI's drug deputation authority. The USMS will not deputize officers to participate in Federal drug investigations.

EFFECTIVE: 01/22/90

31-3 CIVIL LIABILITY

(1) Special Federal Officers are considered Federal employees for purposes of civil suits brought under the Federal Tort Claims Act (FTCA). The FTCA provides that the exclusive remedy for common-law torts committed within the scope of a Federal employee's employment (e.g., a Special Federal Officer) is an action against the United States under the FTCA. Therefore, Special Federal Officers who allegedly commit common-law torts while acting within the scope of their authority as Special Federal Officers cannot be sued in their individual capacities. The suit must be brought against the United States and a resulting judgment for monetary damages, if any, will be satisfied by the United States rather than the individual Special Federal Officer. Specifically, judgments in excess of $2,500 will be paid out of the United States Treasury rather than from FBI appropriations.

(2) Suits brought against a Special Federal Officer for alleged violations of a person's constitutional rights (i.e., Bivens actions) are not brought against the United States but rather against the Special Federal Officer in his/her individual capacity. An adverse judgment for monetary damages, entered against a Special Federal Officer, must be personally satisfied by the Special Federal Officer. However, the Department of Justice (DOJ) may provide legal representation to a Special Federal Officer and may indemnify the officer if it determines that the officer acted within the scope of his/her authority and that representation and indemnification would be in the interest of the United States.

(3) The possibility of civil liability and its potential for adversely impacting on FBI investigations requires that there be tight control and direction over Special Federal Officers. Close supervision of these officers is of critical importance and must be recognized by field office management.

EFFECTIVE: 01/22/90

31-4 GENERAL OR CASE-SPECIFIC AUTHORITY

(1) Generally, the deputation authority granted to a Special Federal Officer is restricted to specifically designated cases. The cases on which a Special Federal Officer is authorized to work are listed by file number on the FD-739 (Oath of Office and Credential - Special Deputation) and FD-739a (Credential Card). The officer is prohibited from assisting on any FBI investigation not reflected on these forms unless doing so under his/her normal police powers. All deputations in Organized Crime Drug Enforcement Task Force (OCDETF) cases are handled on a case-specific basis only. (See MIOG, Part II, 31-5(7)(d).)

(2) There may, however, be situations where general Title 21 investigative authority is justified in non-OCDETF drug investigations.

Often officers are detailed to FBI operational squads on a full time semipermanent basis. These officers occupy FBI space and function much the same as Special Agents. The squads may have a large number of drug cases open and cases are constantly being opened and closed. Under these or similar circumstances a request for general deputation authority may be appropriate. Such justification should be included in the initial deputation request submitted to the SAC.

EFFECTIVE: 08/09/95

31-5 GENERAL ADMINISTRATIVE MATTERS

(1) A deputation request will be approved in only two circumstances:

(a) The officer will be monitoring a Title III;

(b) The officer will be conducting investigation outside his/her own jurisdiction.

(2) When initially deputized, all officers must be sworn in by an SAC, or in his/her absence, an ASAC.

(3) Title 21 deputation authority may be granted by the SAC for a period not to exceed 24 months. Unless otherwise specified,

all FBI deputations automatically expire on October 1st of the second 12 month period in which the deputation was approved by the SAC. This expiration date appears on the FD-739 and FD-739a. EXAMPLE: If an SFO is deputized in June, 1995, that authority may continue, uninterrupted, until October 1, 1996 or for a period of 16 months. Prior to October 1, 1996 that SFO's deputation authority may be renewed, with SAC approval, for an additional 24 months to expire on October 1, 1998. The sponsoring field division is responsible for monitoring deputation expiration dates and for submitting timely renewal requests to the SAC, or in his/her absence, the ASAC.

(4) If the deputation request involves a renewal of an existing deputation authority, the SFO does not need to appear before the SAC, ASAC, or the case Supervisory Special Agent, to be resworn, as long as the deputation is renewed prior to deputation expiration date. A deputation renewal may be accomplished by submitting a timely renewal request to the SAC and having the SAC or, in his/her absence, the ASAC, execute the Deputation Statement on a new FD-739. The officer and SAC or, in his/her absence, the ASAC then subscribe to the Acknowledgement/Oath of Office on the new FD-739. The SAC or ASAC must also sign the FD-739a. This must be accomplished prior to the expiration of the current deputation.

(5) Close supervision of SFOs is of critical importance. The potential for civil liability and adverse impact on investigations is such that it is vital that there be tight control and direction over SFOs and their efforts on the FBI's behalf. (See MIOG, Part II, 31-3(3).)

(6) The following requirements apply to all FBI deputations:

(a) The officer's immediate FBI case supervisor must be identified on the FD-739;

(b) The officer must review the Memorandum to All Employees 6-89, dated 9/27/89, captioned "Principles of Ethical Conduct for Government Officers and Employees." The Manual of Administrative Operations and Procedures (MAOP), Part I, 1-1 (9), may also be used in the absence of this memorandum. The officer should also be advised that he/she will be expected to abide by these standards of conduct for the duration of their deputation and failure to do so may result in the termination of their deputation. (See MIOG, Part II, 31-6(1) (e).)

(c) The officer's deputation authority shall be terminated immediately by the sponsoring field division when it determines that the deputation is no longer necessary, e.g., the officer retires or resigns, is reassigned to other duties, the investigation is closed, etc. The officer must be specifically advised that his/her authority as an SFO is being terminated. The officer's credential card (FD-739a) must be recovered and sent to the SAC as an enclosure to a memorandum notifying the SAC of the termination of the deputation.

(7) The officer will also be required to acknowledge in writing on the FD-739 that he/she has been given instructions set forth below, understands them, and will adhere to them. These instructions are located on the reverse side of copy 3 (white) of the FD-739.

(a) The officer is not to travel out of state on FBI business without being accompanied by a federal Agent unless specifically authorized by an SAC or, in his/her absence, an ASAC.

(b) The officer is not to check federal prisoners out of a federal institution or holding facility unless accompanied by a federal Agent.

(c) The officer is authorized to monitor a federally authorized Title III, acting under the supervision of a federal law enforcement officer.

(d) The officer is deputized only for the specific case(s) authorized in the request for deputation. The officer is not authorized to work on any other federal investigation without specific approval. This deputation is not a general authority to act as a federal Agent.

(e) While this deputation may result in the officer not being liable under Section 1983 actions, the officer is reminded that he/she may nevertheless be liable for BIVENS-type actions.

(f) While engaged in the investigation of cases being directed by the FBI, the officer will remain at all times during the period of this deputation subject to the direction and control of the FBI.

(8) The FD-739a is not intended to be used as a means of primary identification. Any alteration of the FD-739a is specifically prohibited. This includes use of stand-alone credential cases,

photographs, official seals, reproductions, or unauthorized signatures.

(9) By October 1st, of each year, SACs are required to submit annual summary reports, by airtel, captioned "FYXX DEPUTATION SUMMARY REPORT," to the Administrative Unit, Operational Support Section, CID, which identifies all currently approved SFOs.

(a) These summary reports should include the following:

1. Full Name
2. State or Local Agency
3. Date Deputized
4. Expiration Date
5. OCDETF Investigation, file number;
   Non-OCDETF Investigation, file number

EFFECTIVE: 08/09/95

31-6 DEPUTATION REQUEST PROCEDURES

(1) Title 21 Investigations

(a) All deputation requests must be closely coordinated with the U.S. Attorney's Office to ensure compliance and timely completion. All requests should be submitted at least 30 days prior to the time the deputations are required.

(b) The requesting field office must submit a "Title 21 Deputation Request" Memorandum (FD-815), for approval, to the sponsoring field office SAC. The request must have the original signatures of the SAC, case Supervisory Special Agent, and the authorized state or local law enforcement official.

(c) The requesting office must conduct DEA (NADDIS) and FBI (NCIC and field office indices) name checks on all officers to be deputized. The signature of the case Supervisory Special Agent certifies that these name checks have been completed and are negative.

In addition, the signature of the authorized state or local law enforcement official certifies that the officer to be deputized is not the subject of any internal investigations. Finally, the signature of the SAC certifies that the officers to be deputized have been advised of and agree to comply with the instructions set forth in the "Title 21 Deputation Request" Memorandum (FD-815).

(d) Upon approval of the FD-815 by the SAC or, in his/her absence, the ASAC, the requesting office is responsible for preparing the Oath of Office and Credential-Special Deputation (FD-739), securing the appropriate signatures and submitting the FD-739 to the SAC for deputation authority.

(e) The sponsoring office must review the deputation forms for accuracy, particularly file numbers. Any needed corrections should be made and needed descriptive information on the officer obtained. The officer must review the Memorandum to All Employees 6-89, dated 9/27/89, captioned "Principles of Ethical Conduct for Government Officers and Employees." In the absence of this memorandum the MAOP, Part I, 1-1 (9), may be substituted. The officer should be advised that he/she will be expected to abide by these standards of conduct for the duration of his/her deputation and failure to do so may result in termination of their deputation. The name of the officer's FBI case supervisor must be entered in the space provided on the FD-739. (See MIOG, Part II, 31-5(6)(b).)

(f) The instructions located on the reverse side of copy 3 of the FD-739 regarding the officer's responsibilities as an SFO must be given to the officer and acknowledged by signing and dating in the space provided.

(g) When initially deputized, an officer must take the oath of office as presented on the FD-739. The SAC, ASAC, or a Supervisory Special Agent may administer the oath. Both the officer and the SAC or ASAC must sign and date the FD-739 in the spaces provided.

(h) After the FD-739 has been signed by the SAC or ASAC, the FD-739a (Special Deputation Credential) should be detached from copy 3 (white) of the FD-739 and given to the SFO. Copy 1 (blue) of the FD-739 is also given to the SFO. Copies 2 (green) and 3 of the FD-739 should be maintained in the requesting office's deputation control file.

(i) Officers deputized for a non-OCDETF drug investigation do not need to be redeputized in the event the

investigation is converted to the 245 classification.

(2) Non-Title 21 Investigations; Drug Violations Anticipated

(a) Occasionally, deputations may be required for cases not predicated on Title 21 violations; however, Title 21 violations are anticipated. This very narrow category requires deputation by both the FBI and the USMS.

(b) A Non-Title 21; Drug Violations Anticipated, deputation request can be accomplished by following the procedures required for Title 21 investigations and submitting an electronic communication from the SAC, under the caption "FBI Deputation Authority; Non-Title 21 Investigations; Drug Violations Anticipated" to the attention of the Administrative Unit, Operational Support Section, CID. The request must include the following information. (See MIOG, Part II, 31-6 (3)(b).)

1. Identify by title and file number all investigations on which the officer will be working. If general deputation authority is requested, no titles and file numbers are required; however, full justification must be set forth. Note that while an FBI deputation is routinely case specific, USMS deputation authority extends to all federal violations except Title 21.

2. Complete description of the officer, including full name, employing agency, date of birth, social security number, height, weight, sex, race, eye and hair color.

3. Results of field office indices name check, NCIC check, NADDIS check, and a check of the officer's employing agency internal affairs office.

4. U.S. Code violations being investigated.

5. Last firearms qualification date. It must be within the past year.

6. Number of years of law enforcement experience.

7. Contact Special Agent in requesting office.

(c) FBIHQ will prepare a deputation request and forward it to USMS Headquarters. The requesting office (contact

Special Agent) will be contacted by the local USMS office in order to arrange for the deputations.

(d) A copy of the approved FD-815 must accompany the ||electronic communication|requesting Non-Title 21 deputation request.

(3) Non-Title 21 Investigations; Drug Violations Not Anticipated

(a) Officers assisting in investigations which do not involve drug violations are only deputized by the USMS.

(b) The Non-Title 21 Investigation; Drug Violations Not Anticipated deputation request can be accomplished by submitting an|electronic communication|from the SAC, under the caption "FBI Deputation Authority; Non-Title 21 Investigation; Drug Violations Not Anticipated" to the attention of the Administrative Unit, Operational Support Section, CID. The request must include the information set forth in Section 31-6 (2) (b).

(c) FBIHQ will prepare a deputation request and forward it to USMS Headquarters. The requesting office (contact Special Agent) will be contacted by the local USMS office in order to arrange for the deputation.

EFFECTIVE: 05/22/96

|SECTION 32. REWARD POLICY

32-1 REWARDS

A reward is a sum of money or other premium offered by the Government or by a private person for the performance of some special or extraordinary service. By their very nature, offers of rewards are usually made to the public or to a class of persons and, as such, differ from the usual payments to informants set forth in Part I, ||137-8, |of this manual entitled, "Payments to Informants."

EFFECTIVE: 12/20/93

| 32-2 AUTHORIZATION

(1) Authorization to offer and pay rewards is in accordance with current confidential funding guidelines as herein set forth:

(a)	Special Agent in Charge (SAC)	- $20,000
(b)	Section Chief	- $50,000
(c)	Deputy Assistant Director	- $150,000
(d)	Assistant Director	- $250,000
(e)	Associate Deputy Director	- over $250,000

(2) The SAC must approve each reward offer up to $20,000. At the time the reward is paid the field office informant budget will be charged for the amount of the reward payment. If an SAC desires to offer a reward in excess of available funds, he/she will request additional funding and authorization from the appropriate FBIHQ substantive section prior to offering the reward. This communication should specify the amount of the requested reward offer and a detailed justification which addresses 32-4, (1)(a)-(f) below. (See 32-4(4) below.)

EFFECTIVE: 10/07/93

32-3 CRITERIA (See 32-4 below.)

(1) Rewards should only be offered on a selective basis in cases which normally have the following characteristics:

(a) A significant investigation.

(b) Logical avenues of investigation have either been concluded or appear unfruitful.

(c) Individual(s) who may be in possession of useful information are more likely to be motivated by money as opposed to civic duty.

(2) Issues associated with the offering of reward that must be considered are the following:

(a) The legitimate fear that the public offering of a large sum of money could result in the receipt of spurious information and the concomitant need to utilize resources to resolve the truthfulness of the information.

(b) The problem of deciding who is entitled to the reward.

EFFECTIVE: 10/07/93

32-4 REPORTING

(1) Where appropriate, the FBIHQ substantive unit should receive UACB notification of the reward offer under the appropriate case caption setting forth the following information: (See 32-2(2) above.)

(a) A detailed narrative of the investigation.

(b) The amount of the reward to be offered.

(c) Detailed justification which addresses the issues in 32-3 above.

(d) The criteria by which an individual will be considered eligible, i.e., "For information leading to the identification, arrest and conviction of the subject of the investigation," or in a kidnaping matter, "for information leading to the recovery of a kidnaping victim and the identification, arrest and conviction of the persons responsible."

(e) The identities of the local news media by which the reward offer will be made.

(f) The prepared text which will be provided to the local news media.

(2) All reward offers in this regard should be in strict accordance with the instructions set forth in the Manual of Administrative Operations and Procedures, Part II, 5-1, entitled, "Policy and Guidelines for Relations with News Media," and 5-2, entitled, "Contacts with News Media."

(3) The appropriate FBIHQ substantive unit should receive, UACB, airtel notification that a reward recipient has been selected and the basis for the selection.

(4) In those cases where FBIHQ authorization is required, the procedures set forth in 32-2 (2) should be followed.

EFFECTIVE: 10/07/93

32-5 ATTORNEY GENERAL REWARDS FOR INFORMATION CONCERNING ESPIONAGE AND TERRORISM CASES

(1) Title 18, USC, Section 3071, provides the Attorney General with the authority to pay rewards to individuals furnishing information in connection with acts of espionage or terrorism when such information:

(a) leads to the arrest or conviction, in any country, of any individual for the commission of espionage or terrorism against the United States;

(b) leads to the arrest or conviction, in any country, of any individual for conspiring or attempting to commit an act of espionage or terrorism against the United States; or

(c) leads to the prevention, frustration, or favorable resolution (in terrorism cases) of an act of espionage or terrorism against the United States.

(2) The Attorney General determines whether an individual providing information concerning acts of espionage or terrorism is entitled to a reward and the amount of the reward. The maximum reward amount is $500,000. Any reward of $100,000 or more must be approved personally by the President or the Attorney General.

(3) The Attorney General may take such measures in connection with the payment of the reward to ensure that the identities of the recipient and the recipient's immediate family are protected.

(4) No officer or employee of any governmental entity is eligible for any monetary reward under Title 18, USC, Section 3071, if that person provides information concerning espionage or terrorism while in the performance of his or her official duties.

(5) Any individual who furnishes information that justifies a reward by the Attorney General may, in the discretion of the Attorney General, participate in the witness security program.

EFFECTIVE: 04/10/97

SECTION 33. NATIONAL DRUG INTELLIGENCE CENTER (NDIC)

33-1 NATIONAL DRUG INTELLIGENCE CENTER (NDIC)

The NDIC is a multiagency entity operating under the direction of the U.S. Attorney General. The mission of the NDIC is to develop organizational and strategic drug intelligence in support of the U.S. law enforcement community, Intelligence Community, and policy makers. NDIC's mandate necessitates the collection of detailed and relevant information concerning drug enterprises and drug trafficking patterns. On May 4, 1993, the FBI agreed in a Memorandum of Understanding (MOU) to provide NDIC unrestricted access to FBI historical and active investigative information concerning drug trafficking. The following procedures are intended to ensure NDIC's timely access of relevant FBI drug information with appropriate FBI review.

EFFECTIVE: 02/17/94

33-1.1 NDIC Interaction with FBI Field Offices

NDIC may obtain FBIHQ approval to interact directly with FBI field offices.

(1) NDIC will request by written communication FBIHQ approval for NDIC access to specified field offices and FBIHQ elements in furtherance of NDIC's information needs for specified project areas. The Section Chief, Intelligence Section, Criminal Investigative Division (CID) or designee, after consultation with the appropriate operational section, will be responsible for approving NDIC requests.

(2) The affected field offices will be notified by teletype which will detail the scope of NDIC's information needs for specified projects and will include the NDIC point of contact. This teletype will serve as notification of NDIC that their information request has been approved by FBIHQ.

(3) Upon receipt of the teletype, NDIC will communicate directly with the identified FBI field offices and FBIHQ elements. NDIC

will direct copies of all NDIC communications with FBI field offices to the Intelligence Section, CID, FBIHQ.

(4) Significant changes in the scope or direction of the project which impacts on FBI resources will require additional Section Chief, Intelligence Section, CID approval.

EFFECTIVE: 02/17/94

33-1.2 NDIC Analytical Support for FBI Drug Investigations

FBI field offices may receive NDIC analytical support for ongoing FBI drug investigations. The following procedures are in place for field offices desirous of NDIC analytical case support:

(1) The field offices will submit a request to the Sensitive Information Unit, Intelligence Section, CID, by teletype. The teletype should provide an overview of the investigation including the identification of the core organization being addressed.

(2) The Section Chief, Intelligence Section, CID, or designee, after consultation with the appropriate operational section, will review field office requests and prioritize the requests in accordance with the FBI Organized Crime/Drug National Strategy.

(3) Approved requests will be forwarded to NDIC by teletype for their evaluation and determination if sufficient resources are available to support the investigation or project.

(4) Upon NDIC approval of the request, NDIC will notify the field office and FBIHQ by teletype. NDIC will then coordinate the analytical support directly with the field office.

EFFECTIVE: 02/17/94

33-1.3 NDIC Access to FBI Automated Information Systems (AIS)

(1) NDIC will have access to the following FBI AIS:

- Field Office Information Management System (FOIMS)
- FOIMS Telephone data base
- FBIHQ General Index
- Criminal Law Enforcement Application (CLEA)
- Investigative Support Information System

(2) Only a select number of NDIC Intelligence Research Specialists (IRS) will be authorized access to FBI AIS.

(3) The designated IRSs will query the data bases and, when positive results occur, they will make a recommendation concerning the need for other NDIC personnel to see the data.

(4) The data retrieved from the FBI data bases, along with the recommendation, will be reviewed by an FBI Supervisory Special Agent (SSA) detailed to the NDIC. The review will include a finding as to the relevancy of the FBI data to NDIC projects and a determination whether the information should be disseminated to other NDIC personnel.

(5) The NDIC IRSs and SSAs will be subject to the same personnel rules, regulations, laws, and policies applicable to all FBI employees.

EFFECTIVE: 11/25/94

33-1.4 NDIC Access to Informant Files and Grand Jury Material

(1) NDIC will not be provided access to FBI informant files. FBI field offices will determine what level of access NDIC may have to informant information contained in the substantive case files. This is not intended to deny NDIC access to the information, rather it is intended to protect the identities of FBI confidential informants and cooperating witnesses.

(2) NDIC will not be provided access to Grand Jury 6E material unless specifically requested by the field office and in compliance with all applicable 6E rules.

EFFECTIVE: 02/17/94

33-1.5 NDIC Dissemination of FBI Information

NDIC will not disseminate FBI information to other agencies without the concurrence of the Section Chief, Intelligence Section, or designee and in accordance with mutually agreed upon dissemination procedures. The Section Chief of the Intelligence Section, CID or designee will be the FBI approving authority for NDIC dissemination issues.

EFFECTIVE: 02/17/94

33-1.6 NDIC Document Exploitation Branch Service (DocEx)

(1) To further the NDIC's mission of supporting drug law enforcement, the DocEx was created to assist in the storage and analysis of drug-trafficking information obtained through law enforcement activities. The DocEx was established to assist field operations with time-sensitive analysis of information seized pursuant to search warrants, subpoenas, or other enforcement actions which require immediate analysis.

(2) The DocEx Branch consists of Special Agents (SA) and analysts available for travel to field locations to assist in timely analysis of drug-related information. The DocEx is a field support unit and will not conduct unilateral investigations. All information developed by DocEx will be furnished to the field office of the requesting agencies.

DocEx can provide the following services to field offices:

(a) Forensic computer assistance.

(b) Link Analysis of telephone toll records.

(c) Link Analysis of associations and affiliations.

(d) Drug organization profiles.

(e) Financial analysis including identification of assets.

(f) Time-line analysis.

(g) Access to public records databases.

(h) Assistance to search scenes, including electronic inventory, electronic photography, and computer-generated floor plans.

(3) Initial formal requests from FBI field offices for NDIC DocEx assistance should be sent to FBIHQ for approval. A copy of the initial request should be sent to NDIC. It should be in writing, setting forth a brief summary of the investigation, the priority of the investigation within the division and any known requirements concerning the anticipated volume of materials to be seized and the time frames for the enforcement activity. Requests should be forwarded to FBIHQ, Attention: Unit Chief, Intelligence Development Unit, Intelligence Section, Criminal Investigative Division. The NDIC copy should be sent to the National Drug Intelligence Center, 319 Washington Street, Fifth Floor, Johnstown, Pennsylvania 15901, Attention: Chief, Document Exploitation Branch.

(4) The DocEx Branch should be contacted as far in advance of a proposed enforcement operation as possible. This timely notification will ensure that the DocEx team can work with the field offices in order to appropriately plan, staff, and support the timely analysis of seized documents.

(5) After initial coordination between FBIHQ and NDIC, field offices may thereafter correspond directly with NDIC regarding that particular case, keeping FBIHQ informed of any significant developments.

(6) Upon receipt of an approved request at NDIC, a Team Leader (a DEA/FBI SA assigned to NDIC/DocEx) will contact the Field Supervisor or Case Agent for an assessment of the personnel and equipment needed to support an assignment. A Team Leader may also make an on-site assessment, if necessary.

(7) Materials provided to NDIC will be handled solely by the DocEx team and not released to any other agency until approval is obtained from the submitting agency. This is in accordance with policy set forth in the Memorandum of Understanding between the FBI and NDIC. All information developed by DocEx will be returned to the requesting

| agency's field office. |

EFFECTIVE: 01/08/96

SECTION 34. VICTIM/WITNESS ASSISTANCE (VWA)

34-1 INTRODUCTION

The purpose of these MIOG guidelines is to establish procedures to be followed by the Federal Bureau of Investigation (FBI) in responding to the needs of crime victims and witnesses.

EFFECTIVE: 09/08/94

34-2 DEFINITIONS USED THROUGHOUT THESE GUIDELINES

(1) The term "victim" means a person that has suffered direct or threatened, physical, emotional, or pecuniary harm as a result of the commission of a crime, including:

(a) In the case of a victim that is an institutional entity, an authorized representative of the entity, and

(b) In the case of a victim who is under 18 years of age, incompetent, incapacitated, or deceased, one of the following (in order of preference): a spouse; a legal guardian; a parent; a child; a sibling; another family member; or another person designated by the court.

(2) The term "witness" means a person who has information or evidence concerning a crime and provides information regarding his/her knowledge to a law enforcement agency. Where the witness is a minor, the term "witness" includes an appropriate family member or legal guardian.

(3) The term "witness" does not include:

(a) a defense witness; or

(b) an individual involved in the crime as a perpetrator or accomplice.

(4) The term "responsible official" means the Special Agent in Charge (SAC) of the division or his or her designee having the primary responsibility for conducting the investigation.

(5) The term "earliest opportunity" or "earliest possible notice" means one that will not interfere with an investigation or hamper the responsible official in the performance of other law enforcement responsibilities.

(6) The term "multidisciplinary child abuse team" means a professional unit composed of representatives from health, social service, law enforcement, and legal service agencies to coordinate the assistance needed to handle cases of child abuse.

(7) The term "serious crime" (as used in the Victim and Witness Protection Act of 1982 (VWPA)) means a criminal offense that involves personal violence, attempted or threatened personal violence, or significant property loss.

(8) The term "financial" or "pecuniary" harm shall not be defined or limited by a dollar amount, thus the degree of assistance must be determined on a case-by-case basis. For example, since victims' means vary, that which constitutes a minimal financial loss for one might represent a devastating loss for another.

(9) The term "child" means a person who is under the age of 18, who is or is alleged to be:

(a) A victim of a crime of physical abuse, sexual abuse, or exploitation; or

(b) A witness to a crime committed against another person.

(10) The term "child abuse" means the physical or mental injury, sexual abuse or exploitation, or negligent treatment of a child. The term "child abuse" does not include, however, discipline administered by a parent or legal guardian to his or her child provided it is reasonable in manner and moderate in degree and otherwise does not constitute cruelty.

(11) The term "abuse" combined with "physical injury" also means in any case which

(a) a child is dead or exhibits evidence of skin bruising, bleeding, malnutrition, failure to thrive, burns, fracture

of any bone, subdural hematoma, soft tissue swelling, internal injuries, or serious bodily harm; and

(b) such condition is not justifiably explained or may not be the product of accidental occurrence; and

(c) any case in which a child is subjected to sexual assault, sexual molestation, sexual exploitation, sexual contact or prostitution.

(12) The term "local child protective services agency" means that agency of the federal government, of a state, or of a local government that has the primary responsibility for child protection on federal land, or federally contracted or operated facilities.

(13) The term "local law enforcement agency" means any federal, state or local law enforcement agency having primary responsibility for the investigation of an instance of alleged child abuse on federal land, or federally contracted or operated facilities.

(14) The term "mental injury" means harm to a child's psychological or intellectual functioning which may be exhibited by severe anxiety, depression, withdrawal, outward aggressive behavior, or a combination of those behaviors, which may be demonstrated by a change in behavior, emotional response, or cognition.

(15) The term "sexual abuse" includes the employment, use, persuasion, inducement, enticement, or coercion of a child to engage in, or assist another person to engage in, sexually explicit conduct; or the rape, molestation, prostitution, or other form of sexual exploitation of children; or incest with children.

(16) The term "sexually explicit conduct" means actual or simulated:

(a) sexual intercourse, including sexual contact in the manner of genital-genital, oral-genital, anal-genital, or oral-anal contact, whether between persons of the same or opposite sex; sexual contact means the intentional touching, either directly or through clothing, of the genitalia, anus, groin, breast, inner thigh, or buttocks of any person with an intent to abuse, humiliate, harass, degrade, arouse or gratify sexual desire of any person;

(b) bestiality;

(c) masturbation;

(d) lascivious exhibition of the genitals or pubic area of a person or animal;

(e) sadistic or masochistic abuse.

(17) The term "exploitation" means child pornography or child prostitution.

(18) The term "negligent treatment" means the failure to provide, for reasons other than poverty, adequate food, clothing, shelter, or medical care so as to seriously endanger the physical health of a child.

(19) The term "best efforts" means that, in the spirit of full compliance with VWA legislation, Agents and employees engaged in the investigation or detection of a crime shall make their finest attempt to see that victims of crime are accorded the rights described in the Victims Rights and Restitution Act.

EFFECTIVE: 09/08/94

34-3 VWA STATUTORY BACKGROUND

These guidelines combine the requirements of the Victim and Witness Protection Act of 1982 (VWPA), Public Law (PL) 97-291 (October 12, 1982), and the victims rights statutes contained in the Crime Control Act, PL 101-647 (November 29, 1990), which are Title V, Victims' Rights and Restitution Act of 1990 (VRRA); and Title II, Subtitles D and E, Victims of Child Abuse Act of 1990 (VCAA). These laws were enacted to protect and enhance the necessary role of crime victims and witnesses in the criminal justice process, and were further interpreted by the 1991 Attorney General Guidelines for Victim and Witness Assistance (Guidelines). The Guidelines require Department of Justice investigative, prosecutorial and correctional components to make their best efforts to ensure that victims of crime are treated with fairness and respect for the victims' dignity and privacy.

The VRRA sets forth a federal Crime Victims' Bill of Rights which states that a crime victim has the following rights:

(1) The right to be treated with fairness and with respect for the victim's dignity and privacy.

(2) The right to be reasonably protected from the accused offender.

(3) The right to be notified of court proceedings.

(4) The right to be present at all public court proceedings related to the offense, unless the court determines that testimony by the victim would be materially affected if the victim heard other testimony at trial.

(5) The right to confer with attorney for the Government in the case.

(6) The right to restitution.

(7) The right to information about the conviction, sentencing, imprisonment, and release of the offender.

EFFECTIVE: 09/08/94

34-4 ELIGIBILITY FOR VWA

(1) Witnesses (other than defense witnesses and perpetrators or accomplices of the crime) and victims may be considered for assistance through VWA.

(2) In cases where the United States or the public are generally the victims (e.g., narcotics trafficking and tax evasion), victim services will be inappropriate; but in virtually ALL cases, there will be witnesses who will be entitled to witness services.

(3) In Civil Rights cases that allegedly involve police brutality, VWA should not be provided until such time that DOJ assesses the case. In Civil Rights/Inmate cases, VWA will be inappropriate as inmates are already provided medical and mental health services free of charge by the institution in which they are housed.

EFFECTIVE: 09/08/94

34-5 OFFICE FOR VICTIMS OF CRIME (OVC), DOJ

The OVC serves as the federal focal point for all crime victim issues. The Federal Crime Victims Division is one of three divisions within the OVC that is responsible for:

(1) Providing and improving services for victims of federal crime;

(2) Monitoring compliance with legislation pertaining to VWA;

(3) Providing training and technical assistance to federal criminal justice personnel on victim assistance issues.

EFFECTIVE: 09/08/94

34-6 COORDINATION OF VWA MATTERS

(1) FBI Headquarters

(a) All matters pertaining to VWA, which involve the FBI, are coordinated through the Criminal Informant Unit (CIU), Intelligence Section, Criminal Investigative Division (CID), FBI Headquarters (FBIHQ).

(b) The CIU acts in a liaison capacity with FBI field offices; with the OVC, DOJ; with other federal agencies which investigate criminal activity; and with U.S. Attorneys' Offices (USAOs). The CIU coordinates VWA matters, as appropriate, with other CID sections and other divisions at FBIHQ.

(2) FBI Field Offices

(a) Each field office shall have a Victim/Witness Coordinator (VWC) designated by the SAC.

(b) Each division shall advise the CIU, FBIHQ, by airtel of any changes in the designation of the VWC within 10 working days.

(c) Each field office must establish written office policy determining who will perform the following duties:

At the earliest opportunity after the detection of a crime, each Agent and/or VWC shall make reasonable and diligent efforts to:

1. Identify the victims of a crime and inform them of their right to receive, on request, the services described further in these guidelines and;

2. Present the victim with a printed brochure, entitled "Information for Victims and Witnesses of Crime," which will inform each victim of the name, title, business address, and telephone number of the VWC or the Agent to whom such a request for services should be addressed.

a. In Civil Rights cases a pamphlet should not be provided until DOJ accepts the case indicating contributory conduct was not a factor in the brutality.

3. Upon request, after the victim has reviewed the brochure and requests services, the VWC or the Case Agent shall refer the victim to the place where he/she may receive emergency medical and/or social services; compensation for which the victim may be entitled under this or any other applicable law; and the manner in which such relief may be obtained.

a. The VWC or the Case Agent shall, to the extent deemed necessary and feasible, assist in referring the victim to the specific person or office which will provide the above services.

b. The responsible official or his or her designee shall take appropriate action to ensure that any property of a victim that is being held as evidence is maintained in good condition and returned to the victim as soon as it is no longer needed for evidentiary purposes.

4. The VWC or the Case Agent is required to fill out the Victim/Witness Information form for all cases with victims noting if a pamphlet was provided.

5. Consult with and provide the victim or witness with the "earliest possible notice" concerning:

a. the status of the investigation of the crime, to the extent that it is appropriate and will not interfere with the investigation;

b. the arrest of a suspected offender.

6. Upon request by a victim or witness, if cooperation in the investigation of the crime causes his/her absence from work, the VWC or the Case Agent shall notify the employer of the role of the victim or witness in the investigation through verbal or written communication.

7. Upon written request by a victim or witness, if the victim or witness experiences problems with his/her creditors as a result of the victim's or witness' cooperation in the investigation, the VWC or Case Agent shall notify the creditor of the role of the victim or witness in the investigation through verbal or written communication.

EFFECTIVE: 09/08/94

34-7 SECURITY OF COMMUNICATIONS AND FILES

(1) To ensure that appropriate security is afforded communications relating to individuals contacted for VWA purposes, all such communications should be captioned with the individual's true name, followed by the words "VICTIM/WITNESS ASSISTANCE." Bureau regulations regarding the security and release of information is contained in the Manual of Administrative Operations and Procedures (MAOP), Part II, Section 5, 5-1, 5-2; and Section 9, 9-1 through 9-6.

(2) The subclassification number 66F will identify Victim/Witness control files and should be used on all Victim/Witness communications. One copy of each communication should be placed into the control file, one copy in the field office's substantive file, and after the investigation is completed, one copy should be sent to the U.S. Attorney's Office.

(3) The FBIHQ control file number 66F-HQ-1043145 should be used on all written communications being forwarded to FBIHQ.

EFFECTIVE: 09/08/94

34-8 REPORTING DATA RELATIVE TO FBI FIELD OFFICES

EFFECTIVE: 09/08/94

34-8.1 Annual Best Efforts Report

(1) FBI field offices MUST provide FBIHQ with statistics regarding their assistance effort as part of the "Best Efforts Questionnaire" by October 15 of each fiscal year and must include:

(a) The number of criminal cases opened for investigation;

(b) The number of victims involved in these cases;

(c) The number of child victims involved in these cases;

(d) The number of victims assisted by the field office's VWA effort;

(e) The number of witnesses involved in these cases;

(f) The number of witnesses assisted by the field office's VWA effort;

(g) The number of cases in which the VWC was directly involved;

(h) The number of full-time equivalent professional

staff who are dedicated to the VWA effort; and

(i) The types of cases (i.e., white collar, sexual assault, drug-related) that most routinely involve the VWC.

(2) Other issues that concern how well the program is working in the field office should be set forth in the space provided in the "Best Efforts Questionnaire." The information from the "Best Efforts Questionnaire" will be utilized by FBIHQ to prepare the annual "Best Efforts Report" which will be sent to the Attorney General through the OVC. This information will contain all of the aforementioned data for each fiscal year.

(3) In reporting the requirements of the "Best Efforts Questionnaire" to FBIHQ, a letterhead memorandum is to be submitted to the CIU, FBIHQ, by COB October 15 of each fiscal year.

EFFECTIVE: 09/08/94

34-9 FUNDING AND DIRECT SERVICES AVAILABLE TO FEDERAL CRIME VICTIMS

(1) The FBI does not have the authority to provide financial compensation to crime victims but there are various state and local agencies that provide financial and direct assistance to federal crime victims. These services are provided to victims and witnesses by state and local agencies that receive federal crime victim grants from the OVC. The FBI should refer victims and witnesses to all available services. Authority to provide compensation for victims and witnesses rests with each state's compensation board, rather than with the law enforcement departments.

(2) After the victim has reviewed the brochure and if he/she requests services, the VWC or the Case Agent shall refer the victim to the place where he/she may receive emergency medical and/or social services; inform the victim of compensation for which the victim may be entitled under this or any other applicable law; and inform the victim of the manner in which such relief may be obtained.

EFFECTIVE: 09/08/94

34-9.1 State Compensation Programs

(1) Crime victims compensation programs, administered by the states, provide reimbursement of out-of-pocket expenses to victims and survivors of victims of violent crime. Payments are made for medical expenses, including expenses for mental health counseling and care, lost wages attributable to a physical injury, and funeral expenses attributable to a death resulting from a compensable crime. Some other compensable expenses include the replacement of eyeglasses or other corrective lenses, dental services and devices, and prosthetic devices.

(2) The Information Resources Division, Executive Agencies, Personnel and Administrative Support Unit, at FBIHQ has signed a Memorandum of Understanding (MOU) regarding the release of information to state compensation boards. The purpose of this MOU is to expedite the release of information to state compensation boards regarding the verification of an incident reported to the FBI by a crime victim. Each field office has a copy of the MOU and the All SACs airtel related to this MOU.

(3) Each state has its own procedures for crime victim compensation including the determination of maximum award amounts, criteria for approving claims, and the application process.

(4) Each VWC should have a "VICTIM/WITNESS RESOURCE MANUAL." Included in this manual is a complete listing of the contact person(s) for each state compensation board. The VWC shall refer the victim to the contact person who can provide him/her with the necessary information needed to apply for compensation. Compensation information should also be listed on the back of each pamphlet. (Entitled Information for Victims and Witnesses of Crime).

EFFECTIVE: 09/08/94

34-9.2 Crime Victims Fund

The Victims of Crime Act of 1984 (VOCA) established the Crime Victims Fund (Fund) in the U.S. Treasury to provide financial assistance to victim compensation and victim assistance programs. Fines and penalties from convicted federal defendants - not taxpayers - provide the money for the Fund. The major function of the Fund is to make services available to victims of federal crime by providing grants to direct service providers in addition to state compensation boards.

EFFECTIVE: 09/08/94

34-10 THREAT ASSESSMENT

(1) Consistent with the provisions of Title 18, USC, Sections 3521-3528, the responsible official shall make the necessary and appropriate arrangements to enable victims and witnesses to receive reasonable protection against threat, harm, and intimidation from a suspected offender and persons acting in concert with or at the behest of a suspected offender.

(2) Coordination of services for victims/witnesses requesting protection from intimidation should be coordinated through the field office VWC.

(3) If the victim or witness desires formal protection in the Witness Security Program (WSP), the field office VWC or case Agent should contact the Witness Security Program Coordinator in his/her field office who will then take appropriate actions.

EFFECTIVE: 09/08/94

34-11 REPORTING INCIDENTS OF CHILD ABUSE ON FEDERAL LAND AND FEDERALLY OPERATED OR FEDERALLY CONTRACTED FACILITIES

(1) The VCAA was signed into law as Title II of the CCA. Prior to enacting of this legislation, Congress found that incidents of suspected or actual child abuse on federal land, federally operated or federally contracted facilities was grossly underreported and this underreporting is often the result of the lack of a mandatory federal reporting law.

(2) A major function of this Act is to require persons working on federal land, federally operated or federally contracted facilities where children are cared for or reside, who are mandated reporters to report suspected or actual child abuse to the appropriate local law enforcement agency or local child protective service agency.

(3) Failure to file such a report or inhibiting or preventing someone from filing a report results in criminal penalties.

(4) Bureau regulations regarding the reporting of incidents of child abuse in Indian Country is contained in the MIOG, Part I, Section 198-6 through 198-6.9.

EFFECTIVE: 09/08/94

34-11.1 Mandatory Reporting by Federal Investigators

(1) As law enforcement officers, FBI Agents are included in the category of "mandated reporters" as identified in the VCAA. Therefore, any Agent, working on federal land or in federally operated or contracted facilities, where children are cared for or reside, who has knowledge or reasonable suspicion that a child has been or is going to be abused, must immediately notify the local child protective services agency or law enforcement agency of that knowledge or suspicion. Compliance with this law is a responsibility placed upon each Agent INDIVIDUALLY and not on the FBI as an agency.

(2) Any local law enforcement agency or local child protective service agency that receives notification of child abuse or suspected child abuse from a mandated reporter working on federal land or in federally operated or contracted facilities or other individual

must immediately initiate an investigation and take steps to secure the safety and well being of the child (children) involved. This includes the FBI when it has primary investigative responsibility.

(3) When a local law enforcement agency or local child protective services agency receives notification from any person alleging child abuse on federal land or federally operated or contracted facilities outside that agency's primary investigative jurisdiction, the receiving agency must immediately notify the other primary agency and submit a written report within 36 hours as set forth below.

(4) Within 36 hours after receiving notification described above, the receiving agency will prepare a written report that shall include, if available:

(a) the name, address, age and sex of child that is the subject of the report;

(b) the grade and the school in which the child is currently enrolled;

(c) the name and address of the child's parents or other person responsible for the child's care;

(d) the name and address of the alleged offender;

(e) the name and address of the person who made the report to the agency;

(f) a brief narrative as to the nature and extent of the child's injuries, including any previously known or suspected abuse of the child or the child's siblings and the suspected date of the abuse; and

(g) any other information the agency or the person who made the report to the agency believes to be important to the investigation and disposition of the alleged abuse.

(5) Upon completion of their investigation of any allegation of abuse made to a local law enforcement agency or local child protective services agency, such agency shall prepare a final written report on such allegation.

The identity of any person making an initial notification described above shall not be disclosed without consent of that individual to any

person other than a court of law.

EFFECTIVE: 09/08/94

34-11.2 Standard Reporting Form (See MIOG, Part II, 34-11.4.)

In every federally operated (or contracted) facility and on all federal lands, a standard written reporting form, with instructions, shall be disseminated to all mandated reporter groups. Use of this form shall be encouraged, but its use shall not take the place of the immediate making of oral reports, telephonically or otherwise, when circumstances dictate.

EFFECTIVE: 09/08/94

34-11.3 Penalty

(1) Failure to report suspected child abuse may result in a Class B Misdemeanor. Therefore, each Agent must ensure adherence to the statute. The VCAA also states that a "mandated reporter" who makes a report based upon his/her reasonable belief and which is made in good faith, will be immune from civil or criminal liability for making the report.

(2) Since violation of this statute is a misdemeanor, SACs (or their designees) shall inform each Agent of his/her statutory obligation to report and assist in the identification of abused children and discuss the prosecutive merit of each case with the U. S. Attorney before actively investigating complaints.

EFFECTIVE: 09/08/94

34-11.4 Designated Agency to Receive Reports of Child Abuse

(1) The FBI is defined as a "local law enforcement agency" only when it has "primary responsibility for the investigation of an instance of alleged child abuse" on federal land, or federally owned or contracted facilities and must immediately initiate an investigation and take immediate steps to secure the safety and well being of the child (children) involved.

(2) When the FBI receives notification from any person alleging child abuse on federal land, or federally owned or contracted facilities, including Indian country, and the FBI does not have primary investigative jurisdiction as defined by the law, the FBI must immediately notify the appropriate agency and submit a report within 36 hours as set forth in 34-11.2.

EFFECTIVE: 09/08/94

34-11.5 Privacy Protection of Child Witnesses and Child Victims

Stringent procedures for protecting the privacy of a child victim or witness and assuring the confidentiality of information received concerning a child victim or witness, include inter alia: filing under seal all documents which disclose the names of or identifying information concerning child victims and child witnesses, and redacting such names and identifying information from any publicly disclosed documents.

EFFECTIVE: 09/08/94

34-12 TRAINING

(1) It shall be mandatory for the Training Division to provide training to all presently employed and new investigators, concerning their responsibilities in carrying out the provisions of the Victim and Witness Protection Act of 1982, Victims Rights and Restitution Act of 1990, and the Victims of Child Abuse Act of 1990, and to provide written instructions to ensure that these laws are implemented.

(2) The VWA Staff at FBIHQ shall be responsible for coordinating a training curriculum, in conjunction with the Training Division at the FBI Academy, Quantico, with respect to the assistance of victims of and witnesses to federal crime, including child witnesses and victims of child abuse.

EFFECTIVE: 09/08/94

34-12.1 The Multidisciplinary Team Approach in Child Abuse Cases

Each SAC, in coordination with the USAOs, shall provide training to all Agents on multidisciplinary methods of interviewing victims of child abuse and child sexual abuse. The responsible official may follow the criteria, set out in Section 212(b), Subtitle A, Victims of Child Abuse Act (VCAA), recommending that state grant recipients develop and implement multidisciplinary child abuse investigation programs, including:

(1) A written agreement between local law enforcement, social service, health, and other related agencies tocoordinate child abuse investigations;

(2) Joint initial investigative interviews of child victims by law enforcement, health, and social serviceagencies;

(3) A requirement that, to the extent practicable, the same agency representative who conducts an initialinterview, conduct all subsequent interviews; and

(4) Coordination of each step of the investigation

process to minimize the number of the interviews that a child victim must attend.

Where multidisciplinary teams are not yet formally established, federal investigators should coordinatewith existing child protective service agencies to reasonably protect children at risk from further abuse. Compliance with this training requirement shall be included in the agency's annual "Best Efforts Report."

EFFECTIVE: 09/08/94

34-13 RELEVANT EXCERPTS OF THE ATTORNEY GENERAL GUIDELINES ON VICTIM AND WITNESS ASSISTANCE

(1) The following are excerpts relevant to the duties of the FBI regarding VWA as taken from the Attorney General Guidelines for Victim and Witness Assistance. A notation will designate what sections have been skipped.

(2) The Attorney General Guidelines should be interpreted in a positive manner. The advice of FBIHQ should be obtained before the services to victims or witnesses are refused or discontinued if there are any questions regarding the interpretation of these guidelines.

(3) When submitting an inquiry regarding the interpretation of the guidelines or request that the Department of Justice be consulted, provide the necessary information from which a judgment can be made regarding the victim or witness.

ARTICLE I. GENERAL CONSIDERATIONS

A. Statement of Purpose

The purpose of these guidelines is to establish procedures to be followed by the federal criminal justice system in responding to the needs of crime victims and witnesses. These guidelines combine the requirements of the Victim and Witness Protection Act of 1982 (VWPA), PL 97-291 (October 12, 1982), and the victims rights statutes contained in the Crime Control Act of 1990, PL 101-647 (November 29, 1990), "the Act." Consistent with the like purposes of these statutes, the present Guidelines shall provide definitive

guidance on implementation of the 1990 Act as well as continued guidance on the protection of witnesses under the VWPA; and shall serve as a single resource for the Department of Justice (investigative, prosecutorial, and correctional) agencies in the treatment and protection of victims and witnesses of federal crimes.

These Guidelines supersede the 1983 Attorney General Guidelines for Victim and Witness Assistance.

B. Background

The Victim and Witness Protection Act of 1982 was enacted "to enhance and protect the necessary role of crime victims and witnesses in the criminal justice process; to ensure that the federal government does all that is possible within limits of available resources to assist victims and witnesses of crime without infringing on the constitutional rights of defendants; and to provide a model for legislation for state and local governments."

Enactment of the Crime Control Act of 1990 demonstrates the continuing national concern for innocent victims of all crimes and reflects the view that the needs and interests of victims and witnesses had not received appropriate consideration in the federal criminal justice system under the VWPA. The victims' rights provisions of this law mandate that officials of the Department of Justice, and other federal agencies, engaged in the detection, investigation, or prosecution of crime, make their best efforts to ensure that victims of crime are treated with fairness and respect for the victim's dignity and privacy.

The 1990 Victims' Rights and Restitution Act (VRRA) creates, in effect, a federal Victims of Crime Bill of Rights and codifies services that shall henceforth be available to victims of federal crime. This Act does not specifically address the treatment of witnesses; however, it reinforces and augments the VWPA in acknowledging the necessary role of witnesses in the criminal justice process and in ensuring their fair treatment by responsible officials.

The 1990 Victims of Child Abuse Act (VCAA) contains extensive amendments to the criminal code affecting the treatment of child victims and child witnesses by the federal criminal justice system. The 1990 VCAA provides, inter alia, a mandatory requirement for certain professionals working on federal land, or in a federally operated/contracted facility, to report suspected child abuse and child sexual abuse.

Thus, the 1990 victims' rights statutes, i.e., Title V, Victims' Rights and Restitution Act, and Title II, Subtitles D and E, Victims of Child Abuse Act, together with the Victim and Witness Protection Act of 1982, provide the federal criminal justice system with enhanced statutory responsibility to assist and protect crime victims and witnesses in a comprehensive and uniform manner.

C. Application

These Guidelines apply to those components of the Department of Justice engaged in the detection, investigation or prosecution of all federal crimes, and in the detention and incarceration of federal defendants. They are intended to apply in all cases in which individual victims are adversely affected by criminal conduct or in which witnesses provide information regarding criminal activity. While special attention shall be paid to victims of serious, violent crime, ALL victims and witnesses of federal crime who have suffered physical, financial, or emotional trauma shall receive the assistance and protection to which they are entitled under the law.

It should be noted that because of the nature of federal criminal cases it will often be difficult to identify the victims of the offense and, in many cases, there will be multiple victims. Sound judgment will, therefore, be required to make appropriate decisions as to the range of victim services and assistance given. However, Department of Justice personnel should err on the side of providing rather than withholding assistance. For example, in a large-scale federal fraud scheme case, it may be possible to extend victim services and assistance to a representative of the many victims of the fraud.

D. Definitions

For purposes of these Guidelines --

(1) The term "victim" means a person that has suffered direct or threatened, physical, emotional, or pecuniary harm as a result of the commission of a crime, including:

(a) in the case of a victim that is an institutional entity, an authorized representative of the entity; and

(b) in the case of a victim who is under 18 years of age, incompetent, incapacitated, or deceased, one of the following (in order of preference): a spouse; a legal guardian; a parent; a child;

a sibling; another family member; or another person designated by the court.

(2) Federal departments and state and local agencies, as entities, shall not be considered "victims" for the purposes of Articles III and IV of these Guidelines.

(3) The term "witness" means a person who has information or evidence concerning a crime and provides information regarding his/her knowledge to a law enforcement agency. Where the witness is a minor, the term "witness" includes an appropriate family member or legal guardian. The term "witness" does not include a defense witness or an individual involved in the crime as a perpetrator or accomplice.

(4) The term "serious crime" (as used in the VWPA of 1982) means a criminal offense that involves personal violence, attempted or threatened personal violence, or significant property loss.

(5) The term "financial" or "pecuniary" harm shall not be defined or limited by a dollar amount, thus the degree of assistance must be determined on a case-by-case basis. For example, since victims' means vary, that which constitutes a minimal financial loss for one might represent a devastating loss for another.

SKIP D(6), p. 3.

(7) The term "child" means a person who is under the age of 18, who is alleged to be --

(a) a victim of a crime of physical abuse, sexual abuse, or exploitation; or

(b) a witness to a crime committed against another person.

(8) The term "child abuse" means the physical or mental injury, sexual abuse or exploitation, or negligent treatment of a child. The term "child abuse" does not include, however, discipline administered by a parent or legal guardian to his or her child provided it is reasonable in manner and moderate in degree and otherwise does not constitute cruelty.

(9) The term "physical injury" includes lacerations, fractured bones, burns, internal injuries, severe bruising, or serious bodily harm.

(10) The term "mental injury" means harm to a child's psychological or intellectual functioning which may be exhibited by severe anxiety, depression, withdrawal or outward aggressive behavior, or a combination of those behaviors, which may be demonstrated by a change in behavior, emotional response, or cognition.

(11) The term "sexual abuse" includes the employment, use, persuasion, inducement, enticement, or coercion of a child to engage in, or assist another person to engage in, sexually explicit conduct; or the rape, molestation, prostitution, or other form of sexual exploitation of children; or incest with children.

(12) The term "sexually explicit conduct" means actual or simulated--(A) sexual intercourse, including sexual contact in the manner of genital-genital, oral-genital, anal-genital, or oral-anal contact, whether between persons of the same or of opposite sex; sexual contact means the intentional touching, either directly or through clothing, of the genitalia, anus, groin, breast, inner thigh, or buttocks of any person with an intent to abuse, humiliate, harass, degrade, or arouse or gratify sexual desire of any person; (B) bestiality; (C) masturbation; (D) lascivious exhibition of the genitals or pubic area of a person or animal; or (E) sadistic or masochistic abuse.

(13) The term "exploitation" means child pornography or child prostitution.

(14) The term "negligent treatment" means the failure to provide, for reasons other than poverty, adequate food, clothing, shelter, or medical care so as to seriously endanger the physical health of a child.

(15) The term "multidisciplinary child abuse team" means a professional unit composed of representatives from health, social service, law enforcement, and legal service agencies to coordinate the assistance needed to handle cases of child abuse.

ARTICLE II. CRIME VICTIMS' BILL OF RIGHTS

A. Victims' Rights (Sec. 502(a))

BEST EFFORTS TO ACCORD RIGHTS. The Act provides that officers and employees of the Department of Justice and other departments and agencies of the United States engaged in the

detection, investigation, or prosecution of crime shall make their best efforts to see that victims of crime are accorded the rights described in the Act.

BILL OF RIGHTS OF CRIME VICTIMS (Sec. 502(b))

A crime victim has the following rights:

(1) The right to be treated with fairness and with respect for the victim's dignity and privacy.

(2) The right to be reasonably protected from the accused offender.

(3) The right to be notified of court proceedings.

(4) The right to be present at all public court proceedings related to the offense, unless the court determines that testimony by the victim would be materially affected if the victim heard other testimony at trial.

(5) The right to confer with attorney for the Government in the case.

(6) The right to restitution.

(7) The right to information about the conviction, sentencing, imprisonment, and release of the offender.

B. Mandatory Reporting of "Best Efforts"

In the spirit of full compliance with these Guidelines, each United States Attorney, Department Chief of Litigation, FBI Special Agent in Charge (through the Director, FBI) as well as each responsible official of the Department's investigating field offices and correctional facilities, shall report annually to the Attorney General, through the Director, Office for Victims of Crime, by November 1st of each year, on the "Best Efforts" they have made during the preceding fiscal year, in ensuring that victims of crime are accorded the rights set out in the Act.

The responsible official, in preparing the annual "Best Efforts" Report, shall include an account of practices and procedures which have been adopted (and are in actual use in each of their respective offices) during the preceding fiscal year, to provide the services to victims mandated under the Act.

C. Performance Appraisal

The Attorney General strongly recommends that the annual performance appraisal of each federal law enforcement officer, investigator, prosecutor, and corrections officer (and appropriate staff of those agencies) include, as a required activity, implementation of and compliance with the victims' rights and victims and witnesses services provisions set forth in these Guidelines. Institution of this recommendation should be included in the annual "Best Efforts" Report.

ARTICLE III. SERVICES TO VICTIMS AND WITNESSES

As a general rule, for purposes of this Article, Investigative components will be responsible for C(1), (2), and (3), D(1), (2), (3)(a)(b), (5) and (6); prosecutorial components will be responsible for D(3)(c)-(h), and (4); and correctional components will be responsible for D(7) and (8).

Accordingly, at each stage in the performance of services, the transition of responsibility from one component of the Department of Justice to the next must, of necessity, include a sharing of information (in many cases PRIOR to the actual turning over of responsibility). In this way, gaps in notification and other services are eliminated and crime victims receive uniform rather than fragmented treatment, starting from the initial investigation and continuing throughout their entire involvement with the federal criminal justice system.

A. Designation of Responsible Officials (Sec. 503(a))

For purposes of these Guidelines, the Attorney General makes the following designations of persons who will be responsible for identifying the victims of crime and performing the services described in the VRRA, section 503(c), at each stage of a criminal case;

INVESTIGATION

For cases under investigation, and in which no charges have yet been instituted, application of this section will be the responsibility of the following officials:

(1) With respect to offenses under investigation by the Federal Bureau of Investigation, the responsible official shall be

the Special Agent in Charge of the division having primary responsibility for conducting the investigation;

SKIP A. Investigation (2)-(4), Prosecution, Custodial and Corrections, p.7-8.

B. Delegation and Coordination

In order to implement the requirements of the Act, there must be one individual who shall be designated specifically to carry out victim-witness services in each Department of Justice investigating field office and correctional facility, U. S. Attorney's Office, and Justice Department litigating division. This person shall be delegated authority by the responsible official to carry out the activities enumerated in these Guidelines.

It is incumbent upon responsible officials to ensure that all components of the Department of Justice cooperate with each other to the maximum extent possible in providing victims the services to which they are legally entitled. In many instances where certain duties and responsibilities overlap, the responsible officials must take all steps necessary to require coordination and interagency teamwork.

Moreover, all components shall work with appropriate components of other federal agencies that investigate and prosecute violations of federal law to assist them in providing these services to victims; and shall coordinate their victim-witness service efforts with state and local law enforcement officials, including tribal police officials in Indian Country and victim assistance and compensation service providers.

C. Identification of Victims (Sec. 503 (b))

"At the earliest opportunity after the detection of a crime," the responsible official of the investigative agency shall make reasonable and diligent efforts to:

(1) identify the victims of a crime;

(2) inform the victims of their right to receive, on request, the services described in the Act; and

(3) inform each victim of the name, title, business address, and telephone number of the responsible official to whom such

a request for services should be addressed.

Within the meaning of this Article, "the earliest opportunity" means one that will not interfere with an investigation or hamper the responsible official in the performance of other law enforcement responsibilities.

In order to comply with the above informational requirements, it is recommended that a printed brochure, containing general information, brief description of rights and available services as well as the names and phone numbers of key officials and Victim-Witness Coordinator, be given to victims as soon as identified. Whenever possible, personal contact should be initiated with victims. Institution of this recommendation should be included in the annual "Best Efforts" Report.

D. Description of Services (Sec. 503 (c))

(1) "At the earliest opportunity after detection of a crime," the responsible official of the investigative agency shall make reasonable and diligent efforts to inform crime victims concerning:

(a) the place where the victim may receive emergency medical and/or social services;

(b) compensation or restitution for which the victim may be entitled under this or any other applicable law; and the manner in which such relief may be obtained. (see article VI, "Restitution"; see also Appendix, under "Compensation"); and

(c) the availability of public and private programs which provide counseling, treatment and other support to the victim.

(d) The responsible official shall, to the extent deemed necessary and feasible, assist the victim in contacting the specific person or office which will provide the above services.

(2) Consistent with the provisions of Title 18, USC, Sections 3521-3528, the responsible official shall make the necessary and appropriate arrangements to enable victims and witnesses to receive reasonable protection against threat, harm and intimidation from a suspected offender and persons acting in concert with or at the behest of a suspected offender.

Moreover, information on the prohibition against

intimidation and harassment and the remedies therefor shall routinely be made available to victims and witnesses. The responsible official shall, if warranted, advise the component of the Justice Department having the enforcement responsibilities (e.g., the U.S. Marshals Service) of instances involving intimidation or harassment of any victim or witness.

(3) During the investigation and prosecution of a crime, (IF the victim or witness has provided a current address or telephone number) a responsible official shall make diligent and reasonable efforts to consult with and provide the victim or witness "the earliest possible notice" concerning:

(a) the status of investigation of the crime, to the extent it is appropriate and will not interfere with the investigation, including the decision not to seek an indictment or otherwise commence a prosecution;

(b) the arrest of a suspected offender;

SKIP D(3) c-h & D(4), p.10-11.

(5) At all times, the responsible official shall take appropriate action to ensure that any property of a victim that is being held as evidence is maintained in good condition and returned to the victim as soon as it is no longer needed for evidentiary purposes.

(6) The Department of Justice-designated responsible official, or the head of another department or agency that conducts an investigation of a sexual assault shall pay, either directly or by reimbursement of payment by the victim, the cost of a physical examination of a victim and the costs of materials used to obtain evidence.

SKIP D(7)-(8), p.11.

ARTICLE IV. OTHER SERVICES

In addition to the services described above, other appropriate assistance should be extended to victims and witnesses, to the extent feasible, as follows:

A. Federal prosecutors shall resist attempts by the defense to obtain discovery of the names, addresses and phone numbers of victims and witnesses. Responsible officials and employees should

also avoid disclosing the names, addresses and phone numbers of victims and witnesses.

In cases involving a witness who has been promised anonymity or who operated in an undercover capacity, federal prosecutors should consult with such witness, and the primary law enforcement agency involved in the case, before disclosing the identity, address, or location of any such witness, and shall not make such disclosure without the consent of the witness and the law enforcement agency.

B. Upon request by a victim or witness, the responsible official should assist in notifying:

- the employer of the victim or witness if cooperation in the investigation or prosecution causes his/her absence from work; and

- the creditors of the victim or witness, where appropriate, if the crime or cooperation in its investigation or prosecution affects his/her ability to make timely payments.

C. Responsible officials should establish programs to assist Department of Justice employees who are victims of crime.

D. Victims and witnesses should be provided information or assistance with respect to transportation, parking, translator services and related services.

SKIP ARTICLE V. Victim Impact Statement, p. 12-13.

SKIP ARTICLE VI. Restitution, p. 13-14.

ARTICLE VII. CHILD VICTIMS' AND CHILD WITNESSES' RIGHTS

A. Statement of Purpose

The Victims of Child Abuse Act of 1990 (VCAA) was enacted in response to the alarming increase of suspected child abuse cases made each year (over 2 million reports each year). In such cases, because the investigation and prosecution of child abuse is extremely complex, too often the system had not paid sufficient attention to the needs and welfare of the child victim, thus aggravating the trauma that the child had already experienced. Therefore, in order to address this nationwide emergency, the 1990 VCAA provides, inter alia, authorization for training and technical assistance to judges, attorneys and others involved in state and federal court child abuse

cases; requires certain professionals to report suspected cases of child abuse under federal jurisdiction; and amends the United States criminal code to ensure protection of children's rights in court and throughout the criminal justice system.

The new landmark procedures codify specific "rights" for children, never before legally recognized in federal court, and allow other important accommodations for children, including: the right of a child to have an adult attendant accompany the child during court testimony; allowance of the use of closed-circuit television and videotaped depositions of children, as alternatives to live, in-court testimony; stringent procedures which protect a child witness' privacy as well as sanctions for violating such procedures; and a requirement disallowing routine competency examinations, except upon written motion that compelling reasons exist, and ruling out age as a compelling reason. The goal of this Article is intended to assist every federal law enforcement officer, investigator, and prosecutor to take necessary and valid action to reduce the trauma to the child victim caused by the criminal justice system while at the same time increasing the successful prosecution of child abuse offenders.

These Guidelines shall serve to ensure full implementation of the VCAA by all investigative, prosecutorial and correctional components of the Department of Justice.

B. Investigation/Interviewing of Child Victims

(1) Reporting and Investigation of Suspected Cases of Child Abuse.

(a) Pursuant to Sec. 226, Subtitle D, VCAA, certain professionals working on federal land, or in a federally operated or contracted facility, in which children are cared for or reside, are required to report suspected child abuse to an investigative agency designated to receive and investigate such reports. The statute provides further that the Attorney General shall designate the agency to receive and investigate these reports of suspected child abuse. By formal written agreement, the designated agency may be a nonfederal agency.

STANDARD REPORTING FORM. In every federally operated (or contracted) facility and on all federal lands, a standard written reporting form, with instructions, shall be disseminated to all mandated reporter groups. Use of this form shall be encouraged, but its use shall not take the place of the immediate making of oral reports, telephonically or otherwise, when circumstances dictate.

REFERRAL TO LAW ENFORCEMENT. When such reports are received by social services or health care agencies, and involve allegations of sexual abuse, serious physical injury, or life-threatening neglect of a child, there shall be an immediate referral of the report to a law enforcement agency with authority to take emergency action to protect the child. All reports received shall be promptly investigated, and whenever appropriate, investigations shall be conducted jointly by law enforcement and social services personnel (or multidisciplinary team) with a view toward avoiding multiple interviews with the child. In addition, it is important that a child victim be referred for a medical examination, if warranted, by a physician with expertise in forensic examinations.

REPORTING IN INDIAN COUNTRY. As noted earlier, a separate statute, the Indian Child Protection and Family Violence Prevention Act, PL 101-630 (November 28, 1990), governs reporting of child abuse in Indian Country. Pursuant to its provisions, certain professionals are required to report suspected child abuse to the "local law enforcement agency." Title 18, USC, Section 1169. These terms are defined in section 1169 to mean the federal, state or tribal agency that has the primary responsibility for child protection or the investigation of child abuse within the portion of Indian Country involved. Furthermore, where the report indicates the victim or abuser is an Indian and a preliminary inquiry indicates a criminal violation has occurred, the local enforcement agency, if other than the Federal Bureau of Investigation, must report the occurrence immediately to the Federal Bureau of Investigation.

(2) Mandatory Training for all Reporter Groups.

(a) The responsible official of the designated investigative agency shall provide to all mandated reporter groups of covered professionals training in their statutory obligation to report and in the identification of abused children.

(b) Sanctions for Failure to Report. The statute also provides that a covered professional who, while working on federal land or in a federally operated (or contracted) facility, in which children are cared for or reside, learns of facts that give reason to suspect that a child has suffered an incident of child abuse, but fails to report, shall be guilty of a Class B misdemeanor. Title 18, USC, Section 2258.

(3) Interviewing Procedures to Reduce Trauma to Child.

The responsible official, in coordination with the U. S. Attorney, shall provide training to all federal investigators on multidisciplinary methods of interviewing victims of child abuse and sexual child abuse. The responsible official may follow the criteria, set out in Sec. 212(b), Subtitle A, VCAA, recommended for state grant recipients to develop and implement multidisciplinary child abuse investigation programs including:

- a written agreement between local law enforcement, social service, health, and other related agencies to coordinate chid abuse investigation;

- joint initial investigative interviews of child victims by law enforcement, health, and social service agencies;

- a requirement that, to the extent practicable, the same agency representative who conducts and initial interview conduct all subsequent interviews; and

- coordination of each step of the investigation process to minimize the number of interviews that a child victim must attend.

Where multidisciplinary teams are not yet formally established, federal investigators should coordinate with existing child protective service agencies to reasonably protect children at risk from further abuse.

C. Prosecution of Child Abuse Cases

SKIP C(1) - C(3), p.17-21.

(4) Privacy Protection of Child Witnesses and Child Victims.

Stringent procedures for protecting the privacy of a child victim or witness and ensuring the confidentiality of information received concerning a child victim or witness, include inter alia: filing under seal all documents which disclose the names of or identifying information concerning child victims and child witnesses, and redacting such names and identifying information from any publicly disclosed documents.

SANCTIONS FOR VIOLATIONS OF RULE REGARDING DISCLOSURE.

A knowing or intentional violation of the privacy protection accorded children pursuant to Section 3509 of Title 18, USC, is a CRIMINAL CONTEMPT punishable by not more than one year's imprisonment, or fine, or both. Title 18, USC, Section 403.

SKIP C(5) - C(11), p. 22-24

ARTICLE VIII. MANDATORY TRAINING - VICTIMS'/CHILD VICTIMS' AND WITNESSES' RIGHTS

It shall be mandatory for all components of the Department of Justice covered by these Guidelines to provide training to all presently employed and new attorneys, investigators, law enforcement, and corrections officers concerning their responsibilities in carrying out the provisions of the Victim and Witness Protection Act of 1982, Victims Rights and Restitution Act of 1990, and the Victims of Child Abuse Act of 1990, and to provide written instructions to appropriate subcomponents to ensure that these laws are implemented.

In addition, all training units conducted or supported by the Department of Justice shall develop programs which address victim assistance from the perspective of the personnel they train. These units include the FBI Academy at Quantico, the Attorney General's Advocacy Institute, the Federal Law Enforcement Training Center at Glynco, Georgia (through agreement with the U.S. Department of Treasury), and field training conducted by the FBI and DEA.

Compliance with this training requirement shall be included in the agency's annual "Best Efforts" Report.

The Office for Victims of Crime shall be responsible for coordinating training programs, in conjunction with all components of the Department of Justice, with respect to victims and witnesses of federal crime, including child witnesses and victims of child abuse.

ARTICLE IX. NONLITIGABILITY

These Guidelines provide only internal Department of Justice guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any person in any matter civil or criminal. These Guidelines shall not be construed to create, enlarge, or imply any duty or obligation to any victim, witness or other person for which the United States or its employees could be held liable in damages. Nor are any limitations hereby placed on otherwise lawful litigative prerogatives of the Department of Justice.

| Signed August 6, 1991, by Dick Thornburg, Attorney General.|

EFFECTIVE: 09/08/94

SECTION 35. FBI AUTOMATED DATA PROCESSING AND TELECOMMUNICATIONS (ADPT) SECURITY POLICY

35-1 PURPOSE (See MIOG, Part I, 261-2.)

The purpose of this document is to establish uniform policy, responsibilities, and authorities for the implementation of the FBI's Automated Data Processing and Telecommunications (ADPT) Security Program.

EFFECTIVE: 07/26/95

35-2 ADPT SECURITY PROGRAM REFERENCES

References to various regulations/laws applicable to the responsibilities of ADPT security-related personnel are located in Section 35-11.

EFFECTIVE: 07/26/95

35-3 DEFINITION OF TERMS

A glossary of terms is included as Section 35-12.

EFFECTIVE: 07/26/95

35-4 SCOPE

(1) The provisions of this policy apply to all FBI personnel, all FBI ADPT systems, networks and support facilities, and to contractors acting on behalf of the FBI. This policy also applies to any outside organizations, or their representatives, who are granted access to the FBI's ADPT system resources, such as other federal agencies and Joint Task Force members.

(2) Microprocessors which are embedded in and dedicated strictly to production/process control, such as laboratory equipment, are excepted.

(3) The Information Systems Security Unit (ISSU), Security Countermeasures Section, National Security Division, is the point-of-contact for questions concerning this policy document.

EFFECTIVE: 07/26/95

35-5 BACKGROUND

(1) The FBI develops a strategic plan each year which represents a commitment to carry out its mission with increasing effectiveness and efficiency. Information technology is an essential supporting element to the FBI's mission. Employees worldwide use ADPT systems for all facets of the Bureau's operations. These ADPT services also support law enforcement personnel and agencies outside the FBI.

(2) In keeping with the FBI's mission, the goal of the FBI's ADPT security program is to establish and maintain effective security countermeasures to ensure the data confidentiality, integrity, and operational availability of all FBI ADPT systems that process, store, or transmit classified and sensitive but unclassified (hereafter referred to as sensitive) information. In essence, this policy applies to all FBI Systems, given that all Bureau information is treated as at least sensitive. Moreover, Bureau information is not releasable except through the Freedom of Information/Privacy Acts (FOI/PA) process.

(a) The Bureau's ADPT security program has been

designed to address the compromise of information processed in ADPT systems: (a) through penetration by hostile intelligence services and/or criminal elements; (b) by otherwise legitimate users who gain access to data or processes for which they are not authorized; or (c) as a result of inadequate security design, implementation, or operation.

(b) The security countermeasures must preserve the integrity of the information processing to ensure the data is accurate and relevant to achieve the FBI's investigative, law enforcement, and administrative support requirements. Inaccurate data could lead to uninformed decisions and adversely impact the FBI's mission.

(c) Required ADPT services should be available to authorized users within their operational time constraints. The security controls should also make the services unavailable to unauthorized users.

(3) The scope of this policy document is ADPT security, including applicable life cycle security requirements. Several related programs should be taken into consideration when establishing and reviewing ADPT security requirements. Policies and procedures covering the related programs listed below are in this policy by reference (see Section 35-11) and should be obtained by contacting the appropriate program manager.

(a) The Security Countermeasures Section (SCMS), National Security Division (NSD) prescribes policy, procedures, and specifications for maintaining facility security for the FBI. The SCMS is also responsible for the FBI's information security, personnel security, and industrial security programs.

(b) The FBI Central Office of Record (FBICOR) is responsible for setting policy for handling FBI communications security (COMSEC) materials and equipment and for establishing standards and procedures for granting authorization to FBI employees for access or use of those materials and equipment. The FBICOR also evaluates and approves cryptography and communications security measures to be used in ADPT systems.

(c) The Freedom of Information-Privacy Acts (FOIPA) Section, Information Resources Division sets policy for the FBI's FOIPA programs.

EFFECTIVE: 07/26/95

35-6 GENERAL POLICY

(1) Classified and sensitive information in FBI ADPT systems must be safeguarded against unauthorized disclosure, modification, access, use, destruction, or delay in service. An FBI ADPT system is a telecommunications or automated information system that is owned, leased, or operated by or on behalf of the FBI.

(2) The minimum security requirements identified in this policy shall be implemented to protect classified and sensitive information processed, stored, or transmitted by FBI ADPT systems and to protect FBI ADPT system resources.

(3) All ADPT systems processing, storing, or transmitting classified or sensitive information must be submitted for accreditation. Prior to processing, storing, or transmitting classified information, ADPT systems must be accredited. (See Section 35-8.2.) ADPT systems used to process, store, or transmit sensitive information must be accredited as expeditiously as possible.

(4) Connectivity is prohibited between internal FBI ADPT systems and all other systems or networks not covered under the FBI's management authority without approval of the appropriate FBI accrediting authority.

(5) All FBI ADPT systems are for official business only. System users have no expectation of privacy while utilizing these resources.

EFFECTIVE: 07/26/95

35-7 ROLES AND RESPONSIBILITIES

(1) The Director, FBI, is responsible for the security of all ADPT systems under his purview and authorizes the implementation of ADPT security countermeasures based on national policy and guidance. The Director is also responsible for:

(a) Certifying annually to the Department Security Officer (DSO) the adequacy of ADPT systems security in the FBI.

(b) Ensuring a computer security education, training, and awareness program is established in the FBI.

(c) Ensuring all ADPT system security plan documentation is maintained as defined in Section 35-8.1.2.

(d) Designating senior executive service personnel accreditation authority for sensitive and classified computer systems in the FBI. (See (3)(g).)

1. The Assistant Director, NSD, per Director of Central Intelligence Director (DCID) 1/16, has been designated as the accreditation authority for all systems processing, storing, or transmitting sensitive compartmented information (SCI).

2. The Security Programs Manager (SPM), SCMS, NSD, has been designated as the accreditation authority for all classified systems other than those processing, storing, or transmitting SCI, and for all sensitive systems.

(2) The FBI's SPM, SCMS, NSD is responsible for the day-to-day administration of all security programs for the FBI, including the ADPT security program as follows:

(a) Accrediting all classified systems other than those processing, storing, or transmitting SCI and all sensitive systems.

(b) Implementing the FBI's ADPT security education, training, and awareness program on behalf of the Director, FBI.

(c) Submitting security violation reports to the DSO, which include a damage assessment and any actions taken to prevent future violations.

(3) The FBI's ADPT Security Officer, ISSU, SCMS, NSD, has

been appointed by the Director, FBI, to facilitate the implementation of the FBI's ADPT security program, and has the following responsibilities:

(a) Ensuring an operational ADPT security program is in place that asserts a centrally administered security policy. The ADPT security program must comply with the minimum security requirements defined in federal and departmentwide mandates while preserving the flexibility of operations inherent in the Bureau's mission.

(b) Developing and promulgating ADPT security program policy for the FBI. Interpreting policy relating to the FBI ADPT security functions and developing FBI unique guidance as required. Assisting FBI components and their representatives with their efforts to comply with these policies during the performance of their duties, by providing explanation or clarification of ADPT security-related questions that may have an impact on mission performance.

(c) Ensuring the appointment of Computer Systems Security Officers (CSSOs) for classified and sensitive FBI ADPT systems and providing the CSSOs with assistance.

(d) Reviewing and approving acquisitions, in coordination with the CSSO and certifying that the appropriate ADPT security requirements defined in this document are included in the specifications for the operation of an ADPT installation facility, equipment, application system, or acquisition of ADPT hardware, software or related services.

(e) Providing the CSSO with direction and guidance in defining and approving security requirements prior to the start of formal development of software.

(f) Approving the security requirements prior to the start of formal development of software.

(g) Ensuring accreditation packages are prepared for all ADPT systems under FBI authority that process, store, or transmit sensitive or classified information. The contents of an accreditation package are described in Section 35-8.2.

1. Providing guidance on the scope and contents of the system security plans.

2. Reviewing system security plans prepared by or on behalf of the System CSSOs.

3. Preparing statements of residual risk and summary statements of compliance to complete each accreditation package.

4. Submitting the accreditation package to the appropriate accreditation authority, as defined in Section 35-7(1)(d), for accreditation.

5. Acting as a liaison to the DSO and the Department's Justice Management Division, Information Resources Management, Security Programs Manager (IRM-SPM) for all ADPT security matters.

(h) Maintaining a record system containing the status of all accreditation documentation required in this policy document.

(i) Administering the Bureau's security incident reporting program, on behalf of the SPM, to include establishing reporting criteria and coordinating with DOJ.

(j) Coordinating the FBI's virus prevention program, to include: recommending virus prevention solutions; providing guidance in defining the requirements; and selecting the approach.

(k) Conducting ADPT security policy compliance review and oversight activities, as discussed in Section 35-8.4.

(l) Establishing and maintaining a program for conducting periodic facility risk analyses.

(m) Establishing standards and guidance for the preparation of ADPT Installation Disaster and Continuity Plans. Conducting Bureauwide analyses and establishing and verifying Bureau strategies for business recovery and alternate processing. Coordinating the development of ADPT Installation Disaster and Continuity Plans for FBI ADPT facilities.

(n) Establishing standards and guidance for preparing End-User ADPT Contingency Plans.

(o) Identifying areas or issues requiring ADPT security-related research and development effort.

(4) The head of each FBI Division (the Legal Attaches for each Legal Attache office) is responsible for all aspects of ADPT security under his/her jurisdiction. These responsibilities shall be delegated to the Security Countermeasures Program Manager (SCMPM), as set forth in MIOG, Part I, Section 261. In addition, the sponsor of each FBI ADPT system or major application shall ensure that a CSSO is appointed and that this appointment is documented in the system security plan.

(5) The SCMPM shall assume the responsibility for the implementation of ADPT security for a division or Legal Attache. The SCMPM may delegate the day-to-day implementation of the security responsibilities to other members of the division, but will remain the primary point-of-contact for ADPT security matters for the division. Responsibilities include:

(a) Implementing ADPT security policy for ADPT resources that are under the direct operational responsibility of the division.

(b) Enforcing the security policy and ADPT security countermeasures on all personnel who develop, manage, operate, maintain, or use a division's ADPT resources.

(c) Acting as the point-of-contact for security discussions with the FBI's ADPT Security Officer.

(d) Ensuring all employees under his/her jurisdiction receive computer security awareness training, as discussed in Section 35-8.3, following the guidance of the SPM. Promoting general operational ADPT security awareness within his/her organization.

(e) Reporting immediately to the ADPT Security Officer any security incidents, such as any attempt to gain unauthorized access to information, virus infection, or other event affecting the systems security.

(f) Ensuring End User ADPT Contingency Plans are developed, in accordance with Section 35-8.1.4, to ensure continued operations of essential functions within the division in the event that ADPT support is interrupted.

(g) Advising his/her management on implementation of provisions of this policy and applicable references.

(h) Ensuring all ADPT operations are conducted as accredited or that accreditation packages are prepared for operations not covered under existing accreditations. Accreditation is discussed in Section 35-8.2.

(i) Maintaining a list of non-Bureau individuals with access to FBI systems and ensuring whenever a change in SAC occurs, the incoming SAC reevaluates access granted to non-Bureau individuals.

(j) Establish a program that will check on a monthly basis with squads hosting non-Bureau individuals the need for continued access to FBI systems.

(6) A Computer Systems Security Officer (CSSO) shall be assigned for each FBI ADPT system. The CSSO is responsible for:

(a) Ensuring that new ADPT systems, whether acquired or developed, are implemented with appropriate security features and meet the minimum requirements defined in this policy.

1. Defining security requirements prior to starting formal development of a new ADPT system, in coordination with the ADPT Security Officer.

2. Reviewing acquisitions in coordination with the ADPT Security Officer, to ensure that the appropriate ADPT security requirements defined in this policy are included in the specifications of an ADPT installation facility, equipment, application system or acquisition of ADPT hardware, software or related services.

3. Reviewing ADPT systems whenever changes occur, or at least every three years, to ensure changes have not occurred which affect the accreditation status. Conducting design reviews and system tests, and certifying the results recorded, for all new software and for existing software when significant modifications are made. Section 35-8.2 discusses the types of changes that may affect the accreditation status of an ADPT system.

4. Identifying and recommending to management security improvements for the ADPT system.

5. Ensuring that configuration control mechanisms are used and maintained to protect the security-related

features of an ADPT system.

(b) Preparing or overseeing the preparation of system security plans, as discussed in Section 35-8.1, and maintaining the documentation for each ADPT system under his/her assigned responsibility.

(c) Coordinating the preparation and review of the system security plan with the ADPT Security Officer. The required steps in the approval process are discussed in Section 35-8.1.1.

(d) Ensuring the distribution of standard security procedures tailored for end users and operators of computer systems. Advising users of the security features and procedures used on the ADPT system.

(e) Coordinating with the appropriate CSSOs of other systems and/or the FBI's ADPT Security Officer to ensure that planning for shared resources adequately addresses the security requirements that are relevant to each system.

(f) Establishing access control criteria and administrative procedures, which are discussed in Section 35-9.4.1, consistent with Bureau policy, by which only authorized persons can gain access to the ADPT system. The criteria will identify authorized users and identify responsibility for approving all access to the system. The procedures will identify the access control mechanisms and assign responsibility for administering the mechanisms.

(g) Ensuring the review of audit trails and the thorough investigation of audit trail discrepancies, in accordance with the review cycle defined in the system security plan.

(h) Reporting immediately to the Security Countermeasures Program Manager any security incident, such as an attempt to gain unauthorized access to information, virus infection, or other event affecting the system's security.

(7) The Section Chief of the Technical Operations Section, Information Resources Division is responsible for providing policy and guidance on Technical Surveillance Countermeasures (TSCM), intrusion detection, and emanations security.

(8) The Unit Chief of the Network and Information Systems Support Unit (NISSU), Operations Management Section, Information Resources Division is responsible for providing policy and guidance on

the telecommunication-related construction of facilities to meet national standards for emanations security.

(9) All persons who use, manage, operate, maintain, or develop classified or sensitive FBI ADPT systems must comply with this policy.

EFFECTIVE: 11/28/97

35-8 ADPT SYSTEMS SECURITY LIFE CYCLE

(1) This section of the ADPT security policy documents activities relating to ADPT system acquisition and development. Whereas activities pertaining to system development and acquisition have traditionally been centrally conducted by Headquarters elements, the FBI's existing and planned ADPT system technology affords the opportunity for decentralized system development activities. It is imperative that all personnel are aware that, whereas this policy does not discourage systems development, it provides guidance to ensure that ADPT systems that are developed, acquired, and documented are in compliance with this policy.

(2) The topics in this Section are applied as follows:

(a) Security Planning. Security planning activities are the responsibility of the sponsor of an ADPT system, the SCMPM, the CSSO, the ADPT Security Officer, and the SPM. These activities pertain to the development or acquisition of new FBI ADPT systems or modifications to existing systems.

(b) Accreditation. Accreditation activities are the responsibility of the CSSO, the ADPT Security Officer, the SPM, and the accrediting authority.

(c) Security Education, Training, and Awareness. These activities apply to all personnel who manage, use, or operate an FBI ADPT system, whether they are FBI employees or not. These activities are ongoing.

(d) Security Oversight. Security oversight activities related to this policy are conducted by the ADPT Security Officer, the SCMPM, the CSSO, the SPM, and the Inspection Division.

These activities are ongoing.

EFFECTIVE: 07/26/95

35-8.1 Security Planning (See MIOG, Part II, 35-7.)

Security planning activities support the accreditation of all classified and sensitive ADPT systems. This section describes the activities and documentation required to achieve accreditation of a classified or sensitive FBI ADPT system and includes discussion of system security plans, risk management, contingency planning, certification, and system security procedures. The ADPT Security Officer should be consulted prior to the development or acquisition of a classified or sensitive system to establish the scope of the security-related activities and documentation required to achieve accreditation.

EFFECTIVE: 07/26/95

35-8.1.1 Approvals (See MIOG, Part II, 35-7.)

(1) Several steps in the security planning process require the CSSO to seek approvals to proceed with system planning activities.

(2) Security requirements shall be defined and approved by the CSSO and the ADPT Security Officer prior to the start of development or as part of the acquisition process.

(3) The ADPT Security Officer shall approve the system design based on the security reviews prior to the start of system development.

(4) The ADPT Security Officer shall approve the certification test plan and shall approve the results of the certification testing.

(5) DOJ approval of the system security planning

documentation is required prior to accreditation, as discussed in Section 35-8.2.

EFFECTIVE: 07/26/95

35-8.1.2 System Security Plan (See MIOG, Part II, 35-7 & 35-8.2.)

(1) The objective of system security planning is to improve protection of information and information processing resources. The managers most directly affected by and interested in the information or processing capabilities must show that their information and processing capabilities are adequately protected from loss, misuse, unauthorized access or modification, unavailability, or undetected activities.

(2) The boundaries of the computer system must be clearly defined by the CSSO. When a network is used by only the FBI, the FBI ADPT Security Officer will determine the boundaries. Comparable systems, operating in similar environments, may be included in a single system security plan. If additional security measures are required for a particular operating environment, they will be added as a supplement to the system security plan. While generic security plans lessen the administrative burden, CSSOs are responsible for ensuring the ADPT systems under their purview are operating in accordance with the approved system security plan. Local area networks (LANs), hosts with terminals, groups of stand-alone personal computers, workstations, and office automation systems located in the same general area and performing the same general functions, require only one system security plan.

(3) System security plan documentation is required for every classified and sensitive FBI ADPT system. The system security plan documents ADPT security requirements from development or acquisition, implementation, and operation to secure disposal. The system security plan is to be developed and maintained by the CSSO assigned to the ADPT system. The FBI ADPT Security Officer shall define the scope and contents of a system security plan for the FBI ADPT systems to ensure a standardized approach and to ensure compliance with applicable regulations. The system security plan should provide FBI management with sufficient information to make an assessment about the security posture of the ADPT system. The components of a system security plan are:

b2

(a) A security plan which includes the information described in Office of Management and Budget (OMB) Bulletin 90-08 or its successor and is implemented in forms provided by DOJ or using the guidelines for preparing an FBI system security plan. Any questions should be directed to the FBI ADPT Security Officer (ADPTSO), ISSU, SCMS, NSD, [redacted] Room 4282, FBIHQ. The ADPTSO can assist in identifying the mode of operation of the system, assessing the threats and vulnerabilities, estimating the risk involved in the operation, and identifying specific critical countermeasures and/or safeguards. A system security plan form is available in WordPerfect from the ADPTSO.

(b) Documented risk management actions pertaining to the ADPT system. Section 35-8.1.3 discusses the risk management process.

(c) Certification statement that reflects the results of certification tests of the security features applicable to the system. Section 35-8.1.5 discusses the certification process.

(d) Contingency plan which consists of an emergency response plan, backup operations plan, and post-disaster recovery plan. Section 35-8.1.4 discusses the contingency planning process.

(e) Standard security procedures for users and operators of the system. Section 35-8.1.6 discusses standard security procedures.

EFFECTIVE: 07/26/95

35-8.1.3 Risk Management (See MIOG, Part II, 35-8.1.2.)

(1) Risk management is the total process of identifying, controlling, and eliminating or minimizing uncertain risks that may affect system resources. Management must identify the resources to be protected and analyze the risks to determine the appropriate level of protection needed. The risk management process includes: risk analysis, as derived from an analysis of threats and vulnerabilities; management decision to implement security countermeasures and to accept residual risk; implementation and test of selected security countermeasures; and effectiveness reviews.

(2) A risk is derived from the analysis of threats and vulnerabilities. Formal risk analysis requires determining relativity among risks and assessing associated damage or loss. This relativity forms the basis for selecting effective security countermeasures. The FBI does not currently have a standardized methodology for conducting a risk analysis. The DOJ Simplified Risk Analysis Guideline, FIPS PUB 65, and the National Institute of Standards and Technology (NIST) PUB 500-174 provide guidance. The FBI ADPT Security Officer shall be consulted, prior to the start of the risk analysis process, for guidance on the scope of the analysis and the recommended approach to be taken.

(a) Risk analysis will be conducted/sponsored by the ADPT Security Officer for each FBI ADPT mainframe/network facility. The risk analysis procedure will be conducted when a new or substantially modified ADPT facility design is approved and will be conducted:

1. Prior to the approval of design specifications for new general support systems and their supporting installations.

2. Whenever a significant change occurs to the general support system (e.g., adding a local area network; changing from batch to on-line processing; adding dial-up capability). Criteria for defining significant change shall be commensurate with the sensitivity of the data processed by the general support system.

3. At periodic intervals established by the ADPT Security Officer commensurate with the sensitivity of the data processed, but not to exceed every three years if no risk analysis has been performed during that period.

(b) The CSSO shall conduct a risk analysis which focuses on the technical and administrative security control techniques associated specifically with the system under review, including the interface between the operating systems and the application and/or the communications environment and the application and the threats inherent in processing in a specific environment. The results of a facility risk analysis are taken into account when defining and approving security specification for the application systems or network systems.

(3) Responsibility for implementation of the recommendations of a risk analysis rests with the manager of the ADPT

system or facility under review. Response to the recommendations contained in the risk analysis shall include implementation time lines or rationale for nonimplementation of recommended security countermeasures. ADPT system managers must evaluate the recommendations made regarding the systems under review and determine whether to implement the recommendations based on technical and operational feasibility and cost. The FBI's accreditation authority will consider the effects of the reviewer's actions in making accreditation decisions.

EFFECTIVE: 07/26/95

35-8.1.4 Contingency Planning (See MIOG, Part II, 35-7(5), 35-8.1.2.)

(1) Each ADPT system or grouping of like systems must be supported by a logical contingency plan. Well-written contingency plans, routinely reviewed, tested and updated, will enable vital operations and resources to be restored as quickly as possible and keep system downtime to an absolute minimum, providing reasonable continuity of ADPT support if events occur that prevent normal operations.

(2) The elements to be addressed as part of contingency planning for all ADPT systems are:

(a) Emergency response procedures appropriate to fire, flood, civil disorder, natural disaster, bomb threat or any other incident or activity which may endanger lives, property or the capability to perform essential functions.

(b) Backup arrangements, procedures and responsibilities, to ensure that essential (critical) operations can be continued if normal processing or data communications are interrupted for any reason for an unacceptable period of time. The minimally acceptable level of degraded operation of the essential (critical) systems or functions will be identified and prioritized so that the contingency plan accomplishes the priorities.

(c) Post-disaster recovery procedures and responsibilities, to facilitate the rapid restoration of normal

operations at the primary site, or if necessary, at a new facility, following the destruction, major damage or other interruptions at the primary site.

(3) Facility Disaster Recovery Plans address the protection of FBI ADPT general support system security and resources and will ensure the availability of critical Bureau resources, facilitating the continuity of operations during the emergency. The objective of an ADPT Installation Disaster and Continuity Plan is to provide reasonable continuity of computer center/telecommunication information technology support should events occur which prevent normal operations. The ADPT Security Officer is responsible for developing ADPT Installation Disaster and Continuity Plans and defining the testing requirements which will be implemented by the CSSO.

(4) The CSSO shall develop and maintain in a current state, a contingency plan for each ADPT system, which will provide reasonable assurance that critical data processing support can be continued, or resumed quickly, if normal operations of the system are interrupted. The contingency planning activities for an application system are conducted in concert with facility disaster recovery planning and/or end-user contingency planning, when such plans exist. It should be noted that, depending on the results of the criticality assessment, the CSSO for a system may determine that the system is not critical enough to the division or user community to warrant developing and maintaining continuity of operations strategies for interim system processing until normal operations are resumed. In this event, the contingency plan will consist of a continuity of operations statement to that effect. This is subject to the approval of the accrediting authority.

(5) The Security Countermeasures Program Manager for a division is responsible for ensuring that End-User ADPT Contingency Plans are in place for his/her division's microcomputer ADPT resources. The plans also address the division's business continuity requirements for interfacing with applications supported by application contingency plans. The ADPT Security Officer provides guidance for the formulation of the plans. End-User ADPT Contingency Plans are to be developed and/or reviewed and updated periodically or whenever a major change occurs in the processing environment, which includes the physical site, hardware, software, and/or operating systems.

(6) All plans must be operationally tested at a frequency commensurate with the risk and magnitude of loss or harm that could

result from disruption of information processing support.

EFFECTIVE: 07/26/95

35-8.1.5 Certification (See MIOG, Part II, 35-8.1.2, 35-8.4, 35-9.3.2.)

(1) Certification is the comprehensive security test and evaluation of the technical and nontechnical security features of a computer system and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements. Certification primarily addresses software and hardware security countermeasures, but must also consider procedural, physical, personnel, and emanations security to the extent that these measures are employed to enforce security policy.

(a) Custom developed software - Design reviews and systems tests will be performed, and a certification of the results recorded, for all newly developed software and for existing software when significant modifications are made.

(b) Commercial off-the-shelf software (COTS) - Commercially procured software shall be examined to assure that the software contains no features which might be detrimental to the security of the ADPT system. Security-related software shall be examined to ensure that the security features function as specified.

(2) The CSSO shall oversee or conduct certification tests of the computer system. If resources are available, individuals who conduct the certification testing should be independent of the system's developers. The results of the tests shall be documented in a format such that the tests can be repeated, if required, to achieve the results reflected in the certification report.

(3) The system security countermeasures should be modified to reflect the results of the certification testing, as appropriate.

(4) The extent of certification testing will vary with the security mode of operation of the system.

(a) For dedicated security mode of operation, the certification will focus on the physical, procedural, and personnel security measures that ensure all users have the appropriate clearance, access approval, and need-to-know for all data on the system. Since the system is not required to separate users and data with technical security measures, the certification effort will not be extensive.

(b) For the system high-security modes of operation, the certification must cover the same factors as for the dedicated security mode. In addition, testing must establish that the hardware and software security features reliably separate users from any data for which they do not have a need-to-know.

(c) For compartmented and multilevel security modes of operation, specific certification tests will be designed pending DOJ approval (as discussed in Section 35-8.2(1)(b)).

(5) Guidance on conducting these tests shall be provided by the ADPTSO.

EFFECTIVE: 07/26/95

35-8.1.6 Standard Security Practices (See MIOG, Part II, 35-8.1.2.)

System security procedures shall be developed and provided to all users and operators. The procedures shall explain how the security mechanisms in a specific ADPT system work, so that the users and operators are able to consistently and effectively protect their information. The procedures should also be addressed in user training.

EFFECTIVE: 07/26/95

35-8.2 Accreditation (See MIOG, Part II, 35-6, 35-7, 35-8.1.1, 35-9.4, 35-9.4.17.)

(1) Accreditation is an official management authorization to operate an ADPT system: in a particular mode of operation; with a prescribed set of security countermeasures; against a defined threat and with stated vulnerabilities and countermeasures; in a given operational environment; under a stated operational concept; with stated interconnection to other ADPT systems; and, at an acceptable level of risk for which the accrediting authority has formally assumed responsibility. The accrediting authority accepts security responsibility for the operation of an ADPT system and officially declares that a specified system will adequately protect information.

(a) The security processing mode of an ADPT system will be determined based on the classification or sensitivity and formal categories of data and the clearance, access approval, and need-to-know of the users of the system. Formal categories of data are those for which a written approval must be issued before access (for example, SCI compartments or special access programs). The available or proposed security features of the system are not relevant in determining the actual security mode. All ADPT systems will be accredited to operate in one of the following security modes of operation wherein the following statements are satisfied concerning users with direct or indirect access to the ADPT system, its peripherals, remote terminals, or remote hosts:

1. Dedicated Security Mode - all users possess the required personnel security clearance or authorization, formal access approval (if required), and need-to-know for all data handled by the ADPT system.

2. System High-Security Mode - all users possess the required personnel security clearances or authorization, but not necessarily a need-to-know, for all data handled by the ADPT system. If the ADPT system processes classified information, all users must have formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs).

3. Compartmented Security Mode - all users possess a valid personnel security clearance for the most restricted information processed in the computers system; formal access approval for, and have signed nondisclosure agreements for that information to which they are to have access; and a valid need-to-know for that

information to which they are to have access.

4. Multilevel Security Mode - some users do not have a valid personnel security clearance for all the information processed in the ADPT system; all users have the proper clearance and have the appropriate formal access approval for that information to which they have access; and all users have a valid need-to-know for that information to which they are to have access.

(b) The dedicated security mode and the system high-security mode are the only modes of operation authorized by the Department for the processing of classified and sensitive information on ADPT systems. Exceptions to allow the operation of ADPT systems in the compartmented and multilevel security modes may be requested in writing from the DSO by the SPM. (See MIOG, Part II, 35-8.1.5(4).)

(2) All ADPT systems processing, storing, or transmitting classified or sensitive information must be submitted for accreditation. Prior to processing, storing, or transmitting classified information, ADPT systems must be accredited. ADPT systems used to process, store, or transmit sensitive information must be accredited as expeditiously as possible.

(3) The system security plan documentation discussed in Section 35-8.1.2 shall be submitted by the CSSO to the FBI ADPT Security Officer for review. The FBI ADPT Security Officer will develop a summary of compliance with security requirements and a statement of residual risk.

(4) The system security plan, summary of compliance, and statement of residual risk for classified systems must be reviewed by the DSO representative prior to accreditation. For sensitive systems, this documentation will be reviewed by the DOJ IRM-SPM representative prior to accreditation.

(5) The appropriate FBI accreditation authority, i.e., the Assistant Director, NSD, for SCI systems and the SPM for all other systems, makes the accreditation decision based on the summary of compliance, statement of risk, and approved system security plan. The accreditation process results in a decision that the ADPT system is:

(a) accredited to operate, or

(b) given an interim approval to operate for a specific time pending satisfaction of specified requirements, or

(c) denied permission to operate until the identified deficiencies or inadequacies are corrected.

(6) Every FBI ADPT system covered by this policy must be reaccredited every three years. The accreditation status and supporting accreditation documentation shall also be reviewed and revised as appropriate under the following circumstances:

(a) Significant changes in the hardware, software, or data communications configuration that impact security countermeasures defined in the original accreditation package. A significant change constitutes a change that needs to be brought to the attention of the accrediting authority.

(b) Changes in the sensitivity of the information processed.

(c) Changes in the security mode of operation.

(d) Relocation or structural modifications of the computer facility or remote terminal areas.

(e) A breach of security, reported violation of security, or unusual situation that appears to invalidate the accreditation.

(7) The accreditation package revision and review process will include:

(a) Accomplishment of the same steps required for the original accreditation package. Those portions of the package that are still valid need not be redone.

(b) The system security plan, summary of compliance, and statement of residual risk will have to be reviewed and approved by the DOJ IRM-SPM representative or DSO representative, as appropriate.

(c) The appropriate FBI accrediting authority will review and reaccredit the ADPT system.

(8) The FBI ADPT Security Officer shall maintain a record system containing the status of all of the documents in the accreditation packages for the FBI's systems.

(9) The accrediting authority for a system is the only

person authorized to exempt an operation from the security requirements specified in the accreditation statement. This exemption shall be formally documented and shall be retained with the original accreditation package.

EFFECTIVE: 07/26/95

35-8.3 Security Education, Training, and Awareness (See MIOG, Part II, 35-7(5), 35-9.2.)

(1) The ISSU, SCMS, NSD established an ADPT Security Education, Training, and Awareness Program for the FBI. This training shall be extended to all personnel who manage, use, or operate an FBI ADPT system, whether they are employed by the FBI or not. This includes Joint Task Force (JTF) members utilizing any FBI ADPT system (e.g., other federal, state, or local police personnel utilizing FBI microcomputers in an off-site), members of other federal agencies in non-JTF capacity, and any contractor personnel utilizing FBI ADPT systems. The goal of the training program is to ensure that these personnel are made aware of: threats, vulnerabilities, and risks associated with the ADPT systems; what requires protection; information accessibility, handling, marking, and storage considerations; physical and environmental considerations necessary to protect the ADPT system; system, data and access controls; contingency plan procedures; secure configuration control requirements; responsibility to promptly report security violations to the CSSO; and, responsibility to report to the SPM if the security training appears inadequate.

(2) All new employees will receive a security awareness briefing within 60 days of their appointment, as part of their orientation. Continuing training shall be provided whenever there is a significant change in the agency information systems security environment or procedures or when an employee enters a new position which deals with sensitive information. Refresher training shall be given as frequently as determined by the SCMPM, based on the sensitivity of the information that the employee uses or processes. All FBI employees will be provided with refresher awareness material or briefings at least annually.

(3) Each person receiving training shall complete a Notice of Responsibility and Computer Security Awareness Certification

upon completion of each training course which will be retained by the SCMPM. (See Section 35-13.1.) Guidance on the tracking of these training activities will be provided by ISSU, SCMS, NSD.

(4) ADPT security training above the awareness level shall be provided to all personnel who design, implement, or maintain systems regarding the types of security and internal control techniques that should be incorporated into system development, operation and maintenance. The division should consult with the ISSU, SCMS, NSD for guidance on achieving these training objectives.

EFFECTIVE: 07/26/95

35-8.4 Security Oversight (See MIOG, Part II, 35-7(3)(k).)

(1) The ADPT security program is implemented through several policy actions: appointment of CSSOs, acquisition reviews, review and approval of security requirements to support system development; preparation and approval of accreditation documentation; and security incident reporting.

(2) Given the global nature and participation of the FBI ADPT resources, the appointment of CSSOs to assist in ensuring adherence to and to provide a point-of-contact for accomplishing ADPT security activities has been established. CSSOs shall be appointed for all ADPT systems.

(3) The FBI's Inspection Division reviews ADPT security as part of a division's periodic inspection. The FBI ADPT Security Officer will coordinate with the Inspection Division on the status of ADPT security within a division upon completion of the inspection.

(4) Whenever an office makes a major move, e.g., relocates to a new building, the division's Security Countermeasures Program Manager should conduct a compliance review to determine whether the change in physical location has had an impact on the ADPT security posture. The Division's Security Countermeasures Program Manager should consult with the Security Countermeasures Section and should retain the results of the security review as part of the division's security documentation.

(5) As is current practice, the FBI shall continue to

enforce ADPT security as part of the acquisition process. The Information Systems Security Unit must approve ADPT-related acquisitions, as discussed in Section 35-8.1.5. The ISSU should maintain formal records of acquisition activities to ensure that security plans are either developed or modified to reflect the acquisitions. The ADPT Security Officer reviews and approves all ADPT-related acquisitions to certify that the appropriate ADPT security requirements are included in the specification for the operation of an ADPT installation facility, equipment, application system, or acquisition of ADPT hardware, software, or related services. COTRs for a contract action should ensure that the ADPT security-related requirements are adhered to by the contractors throughout the life cycle of the contract.

(6) The ADPT Security Officer shall ensure that periodic system security reviews are conducted. Even if there are no changes to the security posture of a system or division, ADPT systems will be reviewed and reaccredited if three years have elapsed since the date of certification of the security posture. The ADPT Security Officer shall develop, with the assistance of the SPM and the SCMPMs, a list of ADPT systems requiring accreditation. This list should include the recommended priority and the accrediting authority for each ADPT system to be accredited. This list shall be verified annually.

EFFECTIVE: 07/26/95

35-9 MINIMUM SECURITY REQUIREMENTS (See MIOG, Part I, 261-2.)

(1) The goal of ADPT security is to develop a functionally secure, efficient, cost-effective environment based on an assessment of security risks and safeguards. All ADPT systems processing, storing or transmitting classified or sensitive information shall meet the requirements of this policy through automated or manual means. More stringent requirements may be imposed based on a risk analysis. Classified and SCI systems will also conform to the provisions of DCID 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)," 19 July 1988.

(2) This section documents the minimum security requirements for all FBI ADPT systems with respect to facility security, personnel security, administrative security, technical

security features, emanations security, and communications security. Related security disciplines are referenced where appropriate.

EFFECTIVE: 07/26/95

35-9.1 Facility Security

(1) Facility security addresses the requirement to provide physical and environmental security controls commensurate with the level of risk to the ADPT systems supported in a facility, as identified by a risk analysis. The security controls must not be less than the minimum requirements discussed in this section unless a written waiver has been granted by the accrediting authority, i.e., the SPM for non-SCI systems and the Assistant Director, NSD for SCI systems.

(2) For the purposes of this policy, an ADPT facility includes any space housing ADPT equipment such as terminals, microcomputers, mainframe systems, communications equipment and/or supporting environmental control utilities. Facilities also include data storage libraries and ADPT system documentation libraries.

EFFECTIVE: 07/26/95

35-9.1.1 Physical Security

(1) Physical security is that part of the FBI's facility security program which is concerned with the physical measures designed to prevent unauthorized physical access to equipment, facilities, material, information, and documents, and to safeguard them against espionage, sabotage, damage, tampering, theft and other covert or overt acts. ADPT hardware, software, documentation, and all classified and sensitive information handled by the ADPT system shall be protected to prevent unauthorized disclosure, modification, or destruction. ADPT system hardware, software, or documentation shall be protected if access to such resources reveals information that may be used to eliminate, circumvent, or otherwise render ineffective the security countermeasures for classified or sensitive information.

(2) Classified or sensitive FBI information must be processed, stored, or transmitted in spaces which are under exclusive FBI control while operational. When not in operation or under the direct personal control of an authorized person, FBI ADPT systems and information must be protected by storage areas, storage equipment, and/or systems or measures which are consistent with the FBI's facility security program.

(3) The SPM prescribes policies, procedures, and standards for the FBI's facility security program. ADPT security planning must take into consideration the facility security program prior to conducting ADPT operations, at any location, as part of the accreditation process for an ADPT system that processes, stores, or transmits classified or sensitive FBI information.

(4) More stringent physical security controls are required to support the processing, storage, and transmission of SCI. This activity will be subject to the provisions of DCID 1/16 which states the processing of SCI data must be restricted to an accredited SCI Facility (SCIF) and SCI may not be stored on nonremovable storage media except in accredited SCIFs approved for the open storage of SCI. DCID 1/21 provides SCIF physical security criteria. There are instances where other facility security-related rules and requirements apply, too (e.g., the Legal Attaches must comply with Department of State standards in addition to the FBI requirements). ||Network and Information Systems Support Unit (NISSU),|OMS, IRD conducts surveys and develops the specifications for SCIFs and for the field offices and Legal Attaches. These activities are coordinated by the SPM, who is also the accrediting authority for the FBI's SCIFs.

(5) For all types of facilities where classified or sensitive information is stored, processed, or transmitted, physical access will be restricted to those individuals who are cleared and authorized in accordance with the personnel security requirements discussed in Section 35-9.2 and who are necessary to complete job functions and related duties. All uncleared personnel granted facility access must be properly escorted and restricted to those areas necessary to complete their tasks. Classified and sensitive FBI information must be protected from unauthorized disclosure to such persons.

EFFECTIVE: 11/28/97

35-9.1.2 Environmental

(1) Environmental controls address the requirement to provide appropriate temperature and humidity controls, fire protection, power, and natural disaster protection necessary to ensure the continuity of ADPT facilities, equipment, and operations.

(2) An office area that supports desktop ADPT equipment, such as microcomputers, does not require additional environmental controls beyond the requirements specified for human safety and comfort.

(3) ADPT facilities supporting large-scale ADPT operations, such as mainframe computer and telecommunication facilities, require consideration of additional environmental controls as determined by a facility risk analysis. The following additional environmental controls shall be considered.

(a) Fire prevention, detection, suppression and protection measures.

(b) Controls that reduce the risk of water damage, provide water detection, and corrective measures, and water hazard prevention devices.

(c) Electric power supply protection.

(d) Temperature and humidity control.

(e) Natural disaster protection from earthquake, lightning, windstorm, and other natural disasters.

(f) Housekeeping protection from dirt and dust.

(g) Personnel safety features.

EFFECTIVE: 07/26/95

35-9.2 Personnel (See MIOG, Part II, 35-9.1.1, 35-9.4.1, 35-9.4.5.)

(1) All personnel who have been entrusted with the management, operation, maintenance, or use of an FBI ADPT system processing, storing, or transmitting sensitive and/or classified information require the appropriate personnel security approval. The SCMS, NSD, sets policy and provides procedures and guidance in support of the FBI's personnel security program. ADPT security planning must take into consideration the personnel security program prior to conducting ADPT operations as part of the accreditation process for an FBI ADPT system.

(2) All FBI personnel hold Top Secret security clearances. MIOG, Part I, Section 67-7 through 67-7.11, provides policies and procedures for personnel security clearances for Bureau employees.

(3) Non-Bureau personnel who have been entrusted with the management, operation, maintenance, or use of classified FBI ADPT systems require Top Secret security clearances. See MIOG, Part I, Sections 259 and 260. Personnel security approvals for nonclassified FBI ADPT systems are documented in the System Security Plans for these systems.

(4) Non-Bureau personnel who are required to perform maintenance on FBI ADPT systems within FBI controlled space and who do not require access to classified systems may be approved for escorted access based on an FBI-conducted Limited Background Investigation. This activity shall be coordinated by the SPM. Refer to MIOG, Part I, Section 260, "Industrial Security Program," particularly 260-4.1.1.

(5) Personnel must be indoctrinated, as required, prior to being granted access to FBI ADPT systems that support special access programs. The provisions for special access programs are discussed in MIOG, Part II, Section 26-10.2.

(6) ADPT security training must be provided to all personnel who manage, operate, develop or use ADPT systems. Refer to Section 35-8.3.

(7) The SCMPM shall ensure that debriefings are conducted, as required by MIOG, Part I, Section 261-2.

EFFECTIVE: 07/26/95

35-9.3 Technical Security Features (See MIOG, Part II, 35-9.4.2, 35-9.4.6.)

The purpose of this section is to establish near-term requirements and long-term goals to improve the security of the Bureau's ADPT systems through increasing reliance on technical security features. The minimum technical security requirements addressed in Sections 35-9.3.1 and 35-9.3.2 are technically feasible in the Bureau's current ADPT environment and shall be addressed. As technology evolves, the desirable technical security features identified in Section 35-9.3.3 should be addressed during the system planning process.

EFFECTIVE: 07/26/95

35-9.3.1 Minimum Technical Security Requirements (See MIOG, Part II, 35-9.3, 35-9.4.2.)

(1) ADPT systems used for the processing of classified or sensitive information in the System High Security Mode of Operation must have the functionality of the C2 level of trust defined in the Department of Defense (DoD) 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria." The Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, National Computer Security Center Technical Guide 005 (NSC-TG-005), provides guidance on achieving C2 functionality in a network. Other safeguards which maintain the level of system security commensurate with the sensitivity of the data may be substituted in cases where C2 requirements are time-consuming, technically unsound, or adversely affect operations to an unacceptable degree. The Department Security Officer must approve exceptions to C2 for classified systems. The IRM-SPM must approve such exceptions for sensitive systems.

(2) Systems operated in the Compartmented or Multilevel Security Mode of Operation require additional security controls and will be addressed on a case-by-case basis. The ADPT Security Officer shall be consulted to ensure that the technical security requirements

are adequately addressed. These modes of operation require approval by the Department Security Officer.

(3) FBI ADPT operations involving classified information and SCI must be conducted in accordance with the provisions of Director of Central Intelligence Directive 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks." The ADPT Security Officer shall be consulted prior to defining the security requirements for classified and SCI systems to ensure that the technical security requirements defined in DCID 1/16 are adequately addressed.

(4) The design of ADPT systems that process, store, or transmit classified or sensitive information must include, at a minimum, the technical security features discussed in this section. Security countermeasures shall be in place to ensure each person having access to a computer system is individually accountable for his/her actions on the system.

(a) User Identification - The ADPT system shall control and limit user access based on identification and authentication of the user. The identity of each user will be established positively before authorizing access. User identification and password systems support the minimum requirements of access control, least privilege, and system integrity.

(b) Authentication - For ADPT system requiring authentication controls, the ADPT system shall ensure that each user of the ADPT system is authenticated before access is permitted. Currently, use of a password system is the preferred method for authenticating users of FBI ADPT systems. Passwords will be authenticated each time they are used. FIPS PUB 83 provides standards for authentication. More sophisticated authentication techniques, such as retina scanners or voice recognition systems, must be cost-justified through the risk analysis process.

(c) Audit Records - All systems transactions are subject to recording and routine review for inappropriate or illegal activity. Audit trails should be sufficient in detail to facilitate reconstruction of events if compromise or malfunction occurs. Audit trails should be reviewed at least once weekly, or as specified in the system security plan. The audit trail should contain at least the following information:

1. The identity of each user and device having access to the system or attempting to access the system.

2. The time and date of the access, time and date of log-off.

3. Activities that might modify, bypass, or negate security safeguards controlled by the computer system.

4. Security-relevant actions associated with processing.

(d) Object Reuse - All classified and sensitive ADPT systems shall clear memory and storage before reallocation to a different user. This prevents one user from obtaining another user's residual data.

(e) Access Control - For systems operating in the System High Security Mode of Operation, this may be implemented through discretionary access control techniques through measures such as file passwords, access control lists, disk encryption or other techniques, as defined in the approved system security plan. For ADPT systems operating in the compartmented or multilevel security mode, mandatory access control (MAC) is required. MAC is a means of restricting access to information based on labels. A user's label indicates what information the user is permitted to access and the type of access (e.g., read or write) that the user is allowed to perform. An object's label indicates the sensitivity of the information that the object contains. A user's label must meet specific criteria defined by MAC policy in order for the user to be permitted access to a labeled object. This type of access control is always enforced above any discretionary controls implemented by users.

(5) The following additional technical security control requirements apply to FBI ADPT systems:

(a) Internal Labeling - By definition, compartmented mode and multilevel secure modes of operation require internal labeling. In addition, for systems operating in other modes and processing multiple classifications of information (e.g., Sensitive and Secret), security classification labels shall be associated with all data within the system.

(b) Standard Warning Banner - This banner addresses the concerns that those individuals who are using ADPT systems without or in excess of their authority, and those authorized users who are subject to monitoring, be told expressly that by using the system they are consenting to such monitoring. It also provides a basis for

establishing the "knowingly" and "with intent" provisions of Title 18, USC, Section 1030, should prosecution become necessary. The following banner shall be displayed on all FBI ADPT systems at a point prior to the user signing onto the system:

"This FBI system is for the sole use of authorized users for official business only. You have no expectation of privacy in its use. To protect the system from unauthorized use and to insure that the system is functioning properly, individuals using this computer system are subject to having all of their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to the appropriate officials."

(c) Inactivity Time Out - The ADPT system shall lock out an interactive session after an interval of user inactivity not to exceed thirty minutes. The time interval and restart requirements shall be specified in the system security plan.

(6) Interconnections between sensitive and classified FBI ADPT systems and non-FBI ADPT systems must be established through Controlled Interfaces. The ADPT Security Officer must be consulted for guidance on establishing controlled interfaces. The controlled interfaces used in an ADPT system implemented as a network shall be accredited at the highest classification level and most restrictive classification category of information on the network. The controlled interface function of an ADPT system is composed of a combination of gateway and guard functions. Gateways provide a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts, and provide a reliable exchange of security information to allow secure interconnections between components. Automated guard processors and security filters (hereafter referred to as guards) are software or hardware/software techniques or specialized equipment that filter information in a data stream based on associated security labels and/or data content. For example, a guard might accept an input data stream of information of mixed classifications up to SECRET, but permit only data classified up to CONFIDENTIAL to pass.

EFFECTIVE: 07/26/95

35-9.3.2 Security Assurances (See MIOG, Part II, 35-9.3 & 35-9.4.2.)

(1) ADPT systems shall be examined when received from the vendor and before being placed into use.

(a) Hardware - an examination shall result in assurance that the equipment appears to be in good working order and have no "parts" that might be detrimental to the secure operation of the resource when placed under FBI control and cognizance. Subsequent changes and developments which affect security may require additional examination. The emanations security requirements stated in Section 35-9.5 also apply.

(b) Commercial Software - Commercially procured software shall be examined to ensure that the software contains no features which might be detrimental to the security of the ADPT system. Security-related software shall be examined to assure that the security features function as specified.

(c) Software Developed In-house - New or significantly changed software and hardware developed by or specifically for the FBI shall be subject to testing and review at all stages of the development.

(2) The FBI endorses the use of products from the Evaluated Products List (EPL) which is maintained by the National Computer Security Center. Products on the EPL are computer systems, software or components that protect information while it is being stored or processed. They have been evaluated by the government as to the degree of trust that can be placed in them. In order to assess this, the DoD Trusted Computer System Evaluation Criteria was written and products were evaluated against this criteria and given a level of trustworthiness. When certified to be properly implemented through the process discussed in Section 35-8.1.5, these products shall be accepted as meeting the security requirements for the portion of the ADPT system where they are used.

(3) If products from the EPL are not specified or used, a functionality statement is required to discuss how the trusted computing base functionality will be achieved and a time frame for full implementation to the appropriate level of trust will be included. The functionality statement will become part of the accreditation decision. The areas to be addressed in the system security planning phase include:

(a) Confidence in Software Source - In acquiring resources to be used as part of an ADPT system, consideration shall be given to the level of confidence placed in the vendor to provide a quality product, to support the security features of the product, and to assist in the correction of any flaws.

(b) Security Performance Testing - Security performance testing includes both certification testing that is performed before the ADPT system is accredited and ongoing performance testing that is performed on a regular basis.

(c) Flaw Discovery - For ADPT systems operating in the compartmented security mode or multilevel security mode, the vendor shall provide a method for ensuring the discovery of flaws in the system (hardware, firmware, or software) that may have an effect on the security of the ADPT system.

(d) Security Penetration Testing - In addition to testing the performance of the ADPT system operating in the compartmented security mode or multilevel security mode, there shall be testing to attempt to penetrate the security countermeasures of the system. The test procedures shall be documented in the test plan for certification and also in the test plan for ongoing testing.

(e) Description of Trusted Computing Base Protection - The protection and provisions of the trusted computing base shall be documented in such a manner to show the underlying planning for the security of an ADPT system operating in the compartmented security mode or multilevel security mode of operation. The trusted computing base shall be isolated and protected from any user or unauthorized process interference or modification. Hardware and software features shall be provided that can be used to periodically validate the correct operation of the elements of the trusted computing base.

(f) Flaw Tracking and Remediation - For ADPT systems operating in the multilevel security mode of operation, the vendor shall provide evidence that all discovered flaws have been tracked and remedied.

(g) Life-Cycle Assurance - The development of hardware, firmware, and software shall be conducted under life-cycle control and management.

(4) Configuration Management - At a minimum, a configuration management system shall be in place that maintains

control of changes of any of the system's technical features that may alter the accreditation status. Examples include security-related hardware or changes of any line of source or object code of the security-related software. The system will record by whom, for what reason, and when the change is made. Up-to-date documentation of the security-related hardware and/or software design will be maintained. This is a requirement to preserve the integrity of accreditation.

EFFECTIVE: 07/26/95

35-9.3.3 Desirable Technical Security Features (See MIOG, Part II, 35-9.3.)

(1) As technology evolves, system planning should address the achievement of the technical security features addressed in this section. The goal is to achieve a multilevel security mode of operation for all FBI ADPT systems and to provide a trusted path from the workstation forward. A multilevel secure environment allows the FBI to expand the efficiency of information processing. The planning process shall be documented and approved through the system security plan.

(2) Interoperability With External Systems - Support for digital signature standards, nonrepudiation in messaging systems, and data encryption issues should be provided as they relate to interagency communications or interoperability.

(3) Continuous On-Line Automated Monitoring and Warning - The ADPT system shall provide for continuous, real-time monitoring (audit) of use and real-time warning to the CSSO of suspected misuse.

(4) Network Access Control Features - The following areas shall be addressed to achieve a trusted communications path:

(a) Identification and Authentication Forwarding - Reliable forwarding of the identification shall be used between ADPT systems when users are connecting through a network. When identification forwarding cannot be verified, a request for access from a remote ADPT system shall require authentication before permitting access to the system.

(b) Protection of Authenticator Data - In forwarding

the authenticator information and any tables (e.g., password tables) associated with it, the data shall be protected from access by unauthorized users (e.g., by encryption) and its integrity shall be ensured.

(c) Methods of Continuous, On-line Monitoring - Monitoring of network activities shall be included in each network operating in a multilevel security mode. This monitoring shall also include real-time notification to the CSSO of any system anomalies.

(5) Secure Message Traffic - The communications methodology for the network shall ensure the detection of errors in traffic across the network links and the retransmission of erroneous traffic.

(6) Security Label Integrity - For an ADPT system accredited to operate in the compartmented security mode or multilevel security mode, the communications methodology shall ensure: integrity of the security labels; the association of a security label with the transmitted data; and enforcement of the control features of the security labels.

(7) Device Labels - For an ADPT system accredited to operate at the compartmented security mode or multilevel security mode, the communications methodology shall ensure that the originating and destination device labels are a part of each message header and enforce the control features of the data flow between originator and destination.

EFFECTIVE: 07/26/95

35-9.4 Administrative Security and Accountability

(1) Administrative security is the administrative controls and operational procedures used in conjunction with or in place of technical security features to achieve a level of security consistent with the sensitivity of the information processed, stored, or transmitted by FBI ADPT systems. The applicable administrative security controls are documented in the system security plan for a system.

(2) The CSSO shall establish access control criteria and

administrative procedures to control access to information processed, stored, or transmitted by FBI ADPT systems. Access is defined as the ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADPT system. These activities are documented through the system security planning process, approved by the ADPT Security Officer and accredited as discussed in Section 35-8.2.

EFFECTIVE: 07/26/95

35-9.4.1 Access Control Criteria (See MIOG, Part II, 35-7(6), 35-9.4.4.)

(1) The access control criteria shall identify who is authorized to access the system, and identify responsibility for approving all access to the system. The individual who requires access must possess the appropriate security clearance and have the need to know, i.e., access to the information is an operational necessity. Moreover, the system security features must have the technical ability to restrict the user's access to only that information which is necessary for operations and for which the user has clearance.

(2) Bureau personnel accessing internal FBI ADPT systems must have Top Secret security clearances (as discussed in Section 35-9.2). Personnel must only be granted access to systems for which they have a valid need to know based on their operational necessity (e.g., an individual working in the Personnel Division would not require access to case information).

(3) |Non-Bureau individuals operating in|Joint Task Forces (JTF), other federal agencies in non-JTF capacity, and/or private contractors to support particular|operations will be granted limited access to FBI systems. Access will be limited to the privileges assigned to nonsupervisory Special Agent personnel with access to unrestricted case classifications and cases. In limited circumstances, SACs may request supervisory access for non-Bureau individuals who serve as task force supervisors.|

(a) Each request for access must be individually reviewed. The review criteria are:

1. The individual must possess a Top Secret security clearance.

2. The individual must have the need to know, i.e., access to the information is an operational |necessity; SAC/AD recommendation and the |sponsoring division of the application |must concur.|

3. The system security features must have the technical ability to restrict the user's access to only that information which is necessary for operations and for which the user has clearance.

(b) All requests must be submitted in writing to: the sponsoring division of the application, for need-to-know criteria; the SPM, for personnel security clearance status; and, the ADPT Security Officer, for evaluation of the technical security features.

(c) The SPM will be the final adjudicator of all access authorization and will maintain a list of non-Bureau personnel who have been authorized access to FBI ADPT systems.

(4) |The non-Bureau individual must receive Computer Security Awareness Training, Application Training and execute an FBI nondisclosure agreement (FD-868) defined in MIOG, Part II, 35-13.2.|

|(5)| The FBI also operates systems designed for the support of the criminal justice community (e.g., |NCIC).| Because these systems have not been designed for internal FBI use, personnel accountability requirements are defined for each system and are documented in the System Security Plans for these systems. Certain provisions of Section 35-9.4.1 may not apply to these systems.

EFFECTIVE: 08/19/97

35-9.4.2 Administrative Procedures (See MIOG, Part II, 35-13.)

(1) Administrative procedures support the access control mechanisms (i.e., the applicable technical security features discussed in Section 35-9.3) and assign responsibility for administering the mechanisms.

(2) Access control mechanisms provide identification and authentication features as discussed in Section 35-9.3. These features are administered as follows:

(a) Each user of an FBI ADPT system must be uniquely identified. User identification (ID) will not be shared.

(b) Users of FBI ADPT systems will be restricted to only those privileges necessary to perform assigned tasks.

(c) Super-user or system programmer privileges will be granted on a selective basis and will identify any constraints applicable to privileged users.

(d) User accounts that have been inactive for over 90 days will be suspended. The person responsible for administering the access control mechanism is authorized to reinstate such accounts up to 180 days overall. User accounts that have been inactive for 180 days will be deleted and may only be reissued by the person authorized to approve access who is identified in the access control criteria and only to an individual who has been authorized access.

(e) If passwords are selected as the authentication mechanism for a system, password usage shall meet the standards which are set forth in FIPS PUB 112:

1. Passwords shall be changed at least every 90 days.

2. Passwords shall be changed when a security violation is suspected or known.

3. All vendor or default passwords shall be changed prior to system implementation.

4. A password shall be protected commensurate with the information to which it provides access. Password distribution methods shall be provided protection equivalent to the

level of information the passwords protect.

(f) At the time of password issuance, users must be briefed on the following:

1. Password classification and exclusiveness.

2. Measures to safeguard "classified" and "sensitive" passwords.

3. Prohibitions against disclosing passwords to other personnel.

4. Responsibilities for notifying the CSSO of password misuse.

5. Password change procedures.

(3) All systems transactions are subject to recording and routine review for inappropriate or illegal activity. Audit logs should be reviewed as specified in the system security plan. Audit logs should be retained according to the retention period specified in the system security plan. Evidence of security violations must be reported to the ADPT Security Officer. The contents of audit logs are described in Section 35-9.3.1.

(4) When an individual who has been granted access to an FBI ADPT system no longer requires access privileges, the CSSO shall ensure that the individual's identification (ID), passwords, and other access codes are immediately removed from all ADPT systems.

EFFECTIVE: 07/26/95

35-9.4.3 Internal Controls

(1) Office of Management and Budget (OMB) Circular A-123, "Internal Control Systems," prescribes the policies and procedures to be followed by departments and agencies in establishing, maintaining, evaluating and reporting on internal controls in their program and administrative activities. OMB Circular A-123 requires that an organization establish and maintain a cost-effective system of internal controls to provide reasonable assurance that government

resources are protected against fraud, waste, mismanagement, and misappropriation.

(2) Control techniques that support of the internal control objectives for FBI ADPT systems include, but are not limited to the following:

(a) Key duties and responsibilities in authorizing, processing, recording, and reviewing system-related activities should be separated among individuals to the extent practical in the organizational structure. For example, system security-related and general system operational duties should be performed by separate individuals.

(b) Individuals assigned primary responsibility for performing critical functions in support of the ADPT system (e.g., system administration, security administration, system operations, programming, etc.) should have trained alternates who can perform these functions in the event the individual who is assigned primary responsibility is unavailable.

(c) System life cycle documentation should exist to reflect the current state of the ADPT system as it is being operated. The documentation must be sufficient to ensure effective operation by users and system maintenance by programmers.

(3) The risk assessment for the ADPT system should include a review of the susceptibility of the system to waste, loss, unauthorized use, or misappropriation.

EFFECTIVE: 07/26/95

35-9.4.4 Software and Data Security (See MIOG, Part II, 35-13.)

(1) All software used on FBI ADPT systems should be obtained through authorized procurement channels. Use of software acquired through other than appropriate procurement channels (e.g, public domain software, bulletin board services, personally owned software (developed or purchased)) is restricted, must be approved in writing by the SAC as an operational necessity, and must adhere to the applicable software licensing restrictions. Even if the software is approved by the SAC, software acquired through other than the

appropriate procurement channels must be scanned for malicious code and used on a standalone microcomputer to maintain the accreditation of FBI ADPT systems.

(2) FBI microcomputers and associated ADPT storage media which have processed, stored or transmitted other than appropriately acquired software must be cleared prior to processing FBI information. When the software is no longer required, the software should be cleared from the system. Non-FBI microcomputers and associated storage media which have processed, stored, or transmitted non-FBI software and/or information must be sanitized prior to processing, storing, or transmitting any FBI information (e.g., personally owned computer must be sanitized before it is used to process FBI information). The clearing and sanitization processes are discussed in Section 35-9.4.14.

(3) Safeguards must be in place to detect and minimize inadvertent or malicious modification or destruction of an ADPT system's application software, operating system software, and critical data files. The safeguards should achieve the integrity objectives and should be documented in the system security plan. Executable software authorized to run on an FBI ADPT system shall be identified in the system security plan. The level of protection must be commensurate with the sensitivity of the information processed. At a minimum, such media should be backed-up and stored physically separated from the system or at an off-site location.

(4) Virus prevention measures commensurate with the level of risk identified in the risk analysis shall be employed to protect the integrity of the software/data. The ADPT Security Officer manages the virus protection program for the FBI and should be contacted for approved virus scanning and cleanup techniques and/or procedures if there is a suspected or known malicious software threat. Whenever a virus infection is detected, it should be reported to the ADPT Security Officer. All media shall be scanned as follows:

(a) All seized machines and media, prior to introduction to or use by any FBI ADPT system.

(b) All removable magnetic media (such as floppy disks) entering the operational environment regardless of source, prior to use.

(c) All fixed storage devices, on a periodic basis.

(5) Use of software shall comply with copyright laws.

(6) To facilitate compliance with MIOG, Part II, Section 2-9, "Grand Jury (Rule 6)," access to Rule 6(e) information via electronic means must be tracked by user name, date, time, what was accessed, and what actions were taken. All existing Rule 6(e) information readily identifiable as such, and all Rule 6(e) information added to the system must be labeled, as discussed in Section 35-9.4.10, and access to it restricted and tracked, as discussed in Section 35-9.4.1.

(7) Access to SCI information must be restricted to appropriately indoctrinated individuals. Access to TOP SECRET and/or SCI information must be tracked by user name, date, time, what was accessed, what actions were taken. All existing TOP SECRET and/or SCI readily identifiable as such and all TOP SECRET and/or SCI added to the system, must be labeled and access to it restricted. The FBI ADPT Security Officer shall be contacted prior to development or operation of any system processing SCI.

(8) Introduction of data from sources and/or in formats other than those specified in the system security plan (e.g., financial data received from banking institutions) must be approved in writing by the SAC as an operational necessity. These activities must be in conformance with the accreditation of the ADPT system.

(9) In order to maintain software integrity, proper configuration management and change controls must be used to monitor updates to and the installation of software. This process will help to ensure that the software functions as expected and that a historical record of software changes is maintained. Such controls also help to ensure that only authorized software is permitted on the system. These controls may include a software configuration policy that grants managerial approval prior to software modification, then documents the changes.

EFFECTIVE: 07/26/95

35-9.4.5 Maintenance Activities (See MIOG, Part II, 35-13.)

(1) Hardware and software maintenance activity may affect the integrity of existing protection measures or permit the introduction of security exposures into a system (e.g., computer viruses, trojan horses, logic bombs, implant devices, etc.).

(2) All electronic storage and memory devices associated with FBI ADPT systems may not be returned to the vendor for "trade-in" or credit purposes. Exceptions must be approved by the ADPT Security Officer.

(3) Dial-up diagnostic maintenance examination of FBI ADPT equipment via remote communication between vendors and FBI facilities is prohibited.

(4) All maintenance work performed on-site must be supervised by FBI personnel knowledgeable in the operation of the ADPT system regardless of the classification of the system or its associated media. On-site maintenance personnel must meet the personnel security requirements discussed in Section 35-9.2. Vendor diagnostic software used on any FBI microcomputer may not be removed from FBI control. Vendor diagnostic software must be scanned, write-protected, and retained by the Computer Specialist. Only this copy of the software may be used on FBI ADPT systems.

(5) Storage media and microcomputers with nonremovable ADPT storage media must only be transferred through maintenance channels approved by FBIHQ. Only ADPT storage media and microcomputers which have been sanitized and declassified, as discussed in Section 35-9.4.14, can be released from FBI control for maintenance.

EFFECTIVE: 08/04/97

35-9.4.6 Portable Microcomputers (See MIOG, Part II, 35-9.4.17 & 35-13.)

(1) Portable microcomputers (e.g., laptops, notebooks) support the Bureau's mission but require extra attention due to the vulnerability that their portability creates.

(2) As is the case with all FBI equipment, portable microcomputers are considered nonexpendable FBI property. An FD-281 (or FD-281a), "RECEIPT FOR GOVERNMENT PROPERTY," must be executed for portable microcomputers issued to an individual for an extended period of time. Portable microcomputers charged out for shorter periods of time may be accounted for by 0-96, "FBI Property Pass," or an FD-79, "CHARGE-OUT RECORD OF NONEXPENDABLE PROPERTY." See Manual of Administrative Operations and Procedures (MAOP), Part I, 1-3, "GOVERNMENT PROPERTY," for details.

(3) To the extent possible, portable microcomputers should be kept in the possession of the individual to whom they are issued or charged out.

(4) FBI portable microcomputers are authorized to process classified information up to and including Secret/Collateral within the U.S. and its territories and can be connected to the FBI Secure Network (FBINET). The processing of Top Secret and SCI information is not authorized on portable microcomputers without written authorization by the FBI's SPM. Like classified documents, portable microcomputers used to process classified information must be secured in locked storage when not under direct personal control. Portable microcomputers should be kept in the possession of the individual to whom they are issued or charged out. Removable hard drives must always remain in the direct personal control of the individual to whom they are issued or maintained in a secured locked container within FBI-controlled space. The hard drive cannot be left unattended.

(5) All FBI portable microcomputers are to have security subsystems installed which provide specific security features, including individual identification, authentication and access control, and disk encryption, as discussed in Section 35-9.3.

(6) Use of portable ADPT systems outside U.S. territories must be coordinated with the ADPTSO.

(7) Removable hard drive devices used to process, store, or transmit National Security Information (NSI) (this includes all hard drives connected to the FBINET) and/or FBI sensitive information

cannot have communications software that supports the connection to a modem or any other network (LEO, Internet, etc.) without written authorization from the FBI ADPTSO.

(8) Storage of FBI sensitive and/or classified information on removable hard drives must be kept to a minimum. The individual to whom they are issued or charged to will be responsible for ensuring information processed and stored on the removable hard drive is uploaded to the FBI's central record system or transferred to another file storage media which will be retained in controlled FBI space and then deleted from the hard drive. This will reduce the amount of information contained on the hard drive if the drive is lost or stolen.

(9) Portable microcomputers and docking stations are not authorized within the Criminal Informant Management System (CIMS) program.

(10) Connections to non-FBI networks, and the purchase of FAX/MODEMS will be approved, on a case-by-case basis, by the ADPTSO. Portable microcomputers connected to non-FBI networks must operate as DEDICATED microcomputers. These portable microcomputers should not process any FBI sensitive information and MUST NOT process any National Security Information. Additional hard drives can be procured to support the use of FAX/MODEMS.

EFFECTIVE: 08/18/97

35-9.4.7 Inventory of ADPT Systems Processing Classified Information

Computer Specialists must be able to identify all equipment processing, storing, or transmitting classified information, whether operating as part of a network or in a standalone mode of operation. This requirement is in addition to the hardware and software inventory requirements stated in MIOG, Part II, Section 16-18.9.

EFFECTIVE: 08/04/97

35-9.4.8 Telecommunications (See MIOG, Part II, 35-9.4.15 & 35-13.)

(1) Unencrypted dial-up access to FBI ADPT systems is prohibited.

(2) Connections between FBI ADPT systems and non-FBI ADPT systems, public or private, may only be authorized under the following conditions:

(a) Connections to non-FBI ADPT systems for law enforcement-related inquiries (e.g., Department of Motor Vehicles, state or local police departments, and credit bureaus) are authorized. Microcomputers connected to non-FBI networks must operate as dedicated microcomputers. These connections should be documented locally. Documentation should include technical description of the connection and administrative approvals.

(b) All other connections to non-FBI networks will be approved, on a case-by-case basis, by the ADPT Security Officer. For example, FBIHQ is working to provide access from FBINET to U.S. Customs Service, Drug Enforcement Administration, and the National Information Infrastructure (NII). In order to ensure the security of FBINET, these interconnections will require special security measures such as trusted guard processors or multilevel secure systems. As part of the approval process, the ADPT Security Officer will ensure that the appropriate documentation, such as memoranda of understanding, interconnection agreements, etc., is executed on behalf of the FBI.

(3) Because electronic bulletin boards may have constitutional expectations of privacy, a comprehensive program of monitoring electronic bulletin boards for criminal or intelligence purposes is prohibited.

EFFECTIVE: 07/26/95

35-9.4.9 Classification and Controls (See MIOG, Part II, 35-13.)

(1) ADPT systems are classified at the highest level of information that has been entered into, stored on, or processed by the system unless the system can be appropriately declassified. The ADPT system must be labeled, secured and operated commensurate with its classification level. An exception is microcomputers with nonremovable ADPT storage media may only store classified information when the SPM has granted a written waiver for fixed drive open storage and the system is protected with a security system that prevents writing to the fixed drive, forcing use of removable media.

(2) All ADPT storage media containing classified information must be labeled and secured in accordance with the policies for the storage of classified material stated in MIOG, Part II, Section 26-5 through 26-5.3.

(3) FBI ADPT systems that store, process, or transmit sensitive or classified information must be operated only in space that is under exclusive Bureau control and under the personal control of authorized persons. ADPT systems, such as microcomputers, operated under FBI control must be adequately protected to ensure that access to FBI information is available only while FBI personnel are on-site.

(4) When not under the personal control of an authorized person either during or outside regular working hours, FBI microcomputers must be secured as follows:

(a) Microcomputers must be turned off. Exceptions must be approved as part of the accreditation statement.

(b) Diskettes, tapes, removable storage devices and printer ribbons must be labeled and secured commensurate with the highest level of information ever stored on the device.

(5) All FBI ADPT systems connected to FBINET, IISNET, and SAMNET are considered classified and must be appropriately labeled and controlled at the level of those networks.

(6) The FBINET subnetwork is authorized to process up to and including SECRET/collateral data. Under no circumstances may TOP SECRET (TS) or Sensitive Compartmented Information (SCI) be processed by FBINET or introduced by any means into any ADPT system that is connected to the FBINET. To facilitate compliance with this restriction, all correspondence containing TS or SCI levels of data or

information will be "portion marked" to show specific classification levels (i.e., title, paragraph). Portion marking will allow for that information which is classified as SECRET/collateral or below to be entered into ADPT systems accessed by the FBINET network. Under no circumstances may SCI, regardless of classification level, be processed on the FBINET. (See MIOG, Part II, 26-2.6.3.)

EFFECTIVE: 07/26/95

35-9.4.10 External Labels (See MIOG, Part II, 35-9.4.4 & 35-13.)

(1) |All|ADPT storage media must be marked with a classification and a data descriptor|label. Portable microcomputers are exempt from this provision.|

(a) All systems with nonremovable ADPT storage devices must conspicuously display classification and data descriptor labels on the unit that contains the magnetic ADPT storage device. The monitor may also be labeled.

(b) Removable media must be labeled with external markings. An exception to this policy is granted for computer center operations supporting a computerized tape management system that provides internal classification and data descriptor designations, as long as the media remains in FBI-controlled spaces. However, all magnetic media leaving FBI-controlled spaces must be labeled with the external classification and data descriptor labels.

(2) Classification Labels are color-coded labels used to indicate the highest level of classification of information ever stored on ADPT storage media. The classification labels used by the FBI are: CLASSIFIED SCI yellow label, SF-712; TOP SECRET orange label, SF-706; SECRET red label, SF-707; CONFIDENTIAL blue label, SF-708; and UNCLASSIFIED green label, SF-710.

(3) Data Descriptor Labels are used to identify additional safeguarding controls related to information stored on ADPT storage media. They should indicate, at a minimum, the appropriate dissemination and control channels. These labels should also contain information necessary to retrieve archived data. The data descriptor label is SF-711 (or equivalent). The following illustrates information to be inserted on the data descriptor label, as applicable:

(a) Classification - This space should contain either one of the three classification levels: TOP SECRET, SECRET, CONFIDENTIAL; or a statement that the media is either SENSITIVE or UNCLASSIFIED. TOP SECRET, SECRET, or CONFIDENTIAL, and UNCLASSIFIED are defined in MIOG, Part II, Section 26-2.4.

(b) Dissemination - Dissemination restrictions or handling caveats are used in conjunction with certain information to indicate that the information has special access or handling requirements. They are not classification levels. Examples include:

1. Rule 6(e) Material: Rule 6(e) of the Rules of Criminal Procedure, "Secrecy of Proceedings and Disclosure."

2. ORCON: Dissemination and Extraction of Information Controlled by Originator - May not be disseminated outside of the Headquarters of the receiving agency in any form, even extracted or paraphrased, without permission of the originator.

3. NOFORN: Not Releasable to Foreign Nationals - May not be released in any form to foreign governments, foreign nations or non-U.S. citizens without permission of the originator.

(c) Control - Control Channels are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs. Examples of Control Channels are: COMINT Channels (HVCCO) and TK Channels.

(d) Compartments/Code words - A Compartment is one of the divisions into which Sensitive Compartmented Information (SCI) is separated in order to control access, distribution, and protection. SCI is information requiring special Intelligence Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. A special access authorization is required for each compartment. Examples of Compartments are: SI, G, and TK. Multiple Compartments may be handled within a single Control Channel. Generally, each compartment has one or more unique code words associated with it to identify the information as belonging to that compartment. Code words are generally classified and/or handled within specific Control Channels; therefore, no examples are given here.

(e) Agency/Office, Phone, Content, and Comments - The balance of the items on the data descriptor label may be used to

record information pertinent to each division's environment.

EFFECTIVE: 08/18/97

35-9.4.11 Manual Security Classification Reviews

Printouts must be reviewed manually (even if the system initially prints the classification level) to ensure they are appropriately marked with classification and control caveats.

EFFECTIVE: 07/26/95

35-9.4.12 Processing Sensitive Compartmented Information

FBI ADPT operations involving SCI must be conducted in accordance with the provisions of Director of Central Intelligence Directive (DCID) No. 1/16 "Security Policy for Uniform Protection of Intelligence Processed in Automated Systems and Networks." ADPT systems used to process SCI must be housed in accredited Sensitive Compartmented Information Facilities (SCIFs). A list of currently accredited SCIFs is maintained by the SPM. SCI must not be stored on nonremovable ADPT storage media, except in accredited SCIFs approved for the open storage of SCI. The FBI ADPT Security Officer must be contacted prior to the development or operation of any system that will process SCI.

EFFECTIVE: 07/26/95

35-9.4.13 Reuse of Computer System Media

(1) ADPT equipment and storage media that has processed FBI information may only be reused (e.g., transferred to another unit) within FBI control systems (i.e., formal access programs, SCIF, and TEMPEST) after they have been cleared by FBI employees.

(2) The following conditions must be met:

(a) The microcomputer or ADPT storage media remains labeled and secured to the highest level of information ever entered into, stored on, or processed by the device.

(b) When equipment or media is reused by a new user group (e.g., transfer between squads), the ADPT storage media and nonvolatile memory devices must be cleared by the Computer Specialist.

(c) ADPT storage media (removable and nonremovable) may be cleared in the field by FBIHQ approved means as defined by the ADPTSO and approved by the SPM.

(3) Regardless of the clearing process, a microcomputer which has been used to process classified information may not be removed from its operational environment without the written approval of the ADPTSO or the SPM. The microcomputer must continue to be secured commensurate with the highest classification level of information ever entered into, stored on, or processed by the system until the system has been sanitized and declassified.

EFFECTIVE: 08/04/97

35-9.4.14 Disposal of Computer System Media (See MIOG, Part II, 35-9.4.4, 35-9.4.5, 35-9.4.18 & 35-13.)

(1) If the equipment is to be released from the classified control system or disposed of by the FBI, it must first be declassified. Microcomputer equipment which has processed sensitive or classified information may not be released from FBI control until the equipment is declassified (downgraded to UNCLASSIFIED). If the SCMPM cannot formally declassify the microcomputer, release or disposal of the equipment must be through FBIHQ. The following conditions must be met:

(a) Generally, there are two ways to sanitize magnetic media - overwrite or degauss. Overwrite procedures designed to declassify media are stricter than the clearing process designed for use where the media will remain within FBI control systems. Both methods require verification that they were successful. In addition, technological advances in magnetic media may render certain techniques/procedures ineffective. Therefore, the sanitization method must be approved in writing by the SPM.

(b) A microcomputer system may be formally declassified by an original classification authority of the Division after review by the Division Security Countermeasures Program Manager only if all the following conditions are met:

1. The microcomputer system does not contain nonvolatile memory or nonremovable ADPT storage devices.

2. All volatile memory is sanitized by turning off the microcomputer.

3. All removable ADPT storage devices and printer ribbons are removed.

4. The microcomputer is not connected to any FBI network.

(c) When inoperable, diskettes, tape cartridges, printouts, ribbons and similar items used to process sensitive or classified information must be destroyed in accordance with MIOG, Part II, Section 26-15.

(d) When inoperable, hard disks used to process sensitive or classified information must be sent to FBIHQ for proper disposal following procedures provided in MIOG, Part II, Section 26-7.2, pertaining to mail services.

(3) The use of and return of any demonstration systems from vendors must be coordinated with the ADPT Security Officer and the Chief, Property Procurement and Management Section, Finance Division.

EFFECTIVE: 07/26/95

35-9.4.15 Facsimile

(1) Sensitive and classified information should only be transmitted via a secure facsimile system.

(2) Use of facsimile modems on any FBI ADPT system must follow the approval process defined for modems as discussed in Section 35-9.4.8.

EFFECTIVE: 07/26/95

35-9.4.16 Voice Mail Systems

Because there are no recognized standards for voice mail systems, these systems have not been built to meet standard security specifications and are not considered to be secure systems. These systems are, in fact, susceptible to unauthorized access. Therefore, any message left on a voice mail system should contain the minimal amount of information possible. Do not leave any information on a voice mail system that, if compromised, could damage the mission of the FBI or endanger lives. All suspected unauthorized access attempts shall be reported to the SCMPM.

EFFECTIVE: 07/26/95

35-9.4.17 Bureau Work Performed at Home

(1) Use of an FBI portable computer (e.g., laptop, notebook) at home is authorized if usage is in keeping with the policy stated in Section 35-9.4.6.

(2) Use of other ADPT equipment (whether Bureau equipment or personally owned equipment) at home must meet the requirements for all FBI ADPT systems that are discussed in this policy, to include the system security plan, risk analysis, contingency plan, certification, standard security procedures, and accreditation as discussed in Section 35-8.2. Although it is technically feasible to address these requirements, it is generally cost prohibitive to conduct these activities for individual systems. Therefore, use of ADPT equipment to process Bureau work at home is actively discouraged unless it is an operational necessity.

(3) Under the following conditions, the STU-III, Type 1, a secure telephone unit designed specifically for the secure transmission of Sensitive but Unclassified and National Security Information, may be approved by the ADPT Security Staff, NSD, for the installation in an FBI employee's private residence located in the United States only. An electronic communication should be directed to the ADPT Security Officer, NSD, requesting approval.

(a) The Assistant Director in Charge, Assistant Director, or SAC must approve, in writing, the operational need for the installation of a STU-III, Type 1, in the employee's residence.

(b) STU-III, Type 1, installation is approved for the transmission of conversations (voice) up to, and including, Top Secret. No Sensitive Compartmented Information will be approved for transmission from a private residence. This policy does not apply to the transmission of data.

(c) When the STU-III is in an unkeyed state, the equipment must be protected in a manner that is sufficient to preclude any reasonable chance of theft, sabotage, or tampering. When not in use, the Crypto-Ignition Key (CIK) must be locked up or retained in the custody of the authorized FBI employee. The room in which the equipment is installed must prevent eavesdropping. In addition, Sensitive but Unclassified and NSI conversations must be held in the presence of authorized personnel only, that is, personnel with appropriate clearances and need to know. The STU-III must be installed in a room that can meet these requirements.

EFFECTIVE: 08/28/97

35-9.4.18 Use of Non-Bureau-Owned ADPT Systems

(1) Use of personally owned, leased, or loaned equipment (e.g., equipment provided by a local police department as part of a JTF) to support the processing of Bureau information must meet all provisions of this policy. The following additional restrictions apply:

(a) Under no circumstances will personally owned, leased, or loaner equipment or media be used to process classified information.

(b) To the extent possible, information should be stored on FBI-owned storage media. Provisions should be made which allow for FBI retention of nonremovable, nonvolatile storage device (e.g., microcomputer hard drives) if the device cannot be successfully sanitized as discussed in Section 35-9.4.14.

(2) For security reasons, placement and removal of microcomputers and related media to operational environments where classified information is processed must be approved by the responsible Security Countermeasures Program Manager or the FBI Security Programs Manager.

EFFECTIVE: 07/26/95

35-9.5 Emanations Security (See MIOG, Part II, 35-9.3.2.)

(1) ADPT systems, including but not restricted to microcomputers and communications switches, used to process classified information must meet national TEMPEST standards for the specific operational and physical environment in which they are operated. In many instances, these standards may be met with commercial equipment.

(2) The Section Chief of the Technical Operations Section, IRD, provides policy and guidance on Technical Surveillance Countermeasures (TSCM) and emanations security. The Technical

Programs Unit conducts TEMPEST certifications.

(3) |Network and Information Systems Support Unit (NISSU),|OMS, IRD is responsible for ensuring the provisions of NACSIM 5203, "Guidelines for Facility Design and Red/Black Installation (U)," June 30, 1982 and Appendix B to NACSIM 5204, "NSA Specifications for RF Shielded Enclosures for Communications Equipment General Specifications," are met with respect to addressing the telecommunications aspects of this program. |(NISSU)|defines the requirements, develops the specifications and conducts inspections. These activities are coordinated with the SPM.

EFFECTIVE: 11/28/97

35-9.6 Communications Security

The FBI's ADPT security program relies on a related program, the communications security program, to protect telecommunications systems. Communications security (COMSEC) is defined as all measures which are taken to prevent recovery of information while it is being transmitted by telecommunications equipment. All communications circuits used to interconnect remotely located components of FBI ADPT systems which process, store or transmit classified or sensitive information require consideration of COMSEC measures.

EFFECTIVE: 07/26/95

35-10 SECURITY INCIDENTS AND VIOLATIONS

(1) A security incident is a condition that has the potential to impact the security of an ADPT system, such as any attempt to gain unauthorized access to information, virus infection, or loss or theft of computer media. Security incidents may result from intentional or unintentional activities. ADPT security-related incidents should be reported to the FBI ADPT Security Officer by the CSSO or SCMPM, as appropriate. The FBI ADPT Security Officer will address the impact of the security incidents on the system's

accreditation status and recommend additional security countermeasures to reduce generic risks. In addition, DOJ requires that all malicious software incidents of DOJ automated information systems, including mainframes, microcomputers, networks, or personal computers, be documented and reported. For reporting purposes, malicious software incidents include any detection of malicious software, whether detected on magnetic media prior to entry into an FBI ADPT system or after infection of the system, and any actual execution of malicious software. The ADPT Security Officer will maintain the appropriate records and fulfill the DOJ reporting requirements on behalf of the SPM. DOJ will use this information to determine the extent of problems in the Department.

(2) FBI employees are subject to disciplinary action for violation of FBI ADPT security policy. Such violations may invoke FBI disciplinary action even if they are not criminally pursued. Reportable ADPT security-related violations are addressed in the MAOP, Part I, Section 13-13, "Schedule of Disciplinary Offenses and Penalties for FBI Employees," and should be reported as specified in the MAOP. Sanctions for noncompliance are also provided in the MAOP. It should be noted that reporting violations to the ADPT Security Officer does not relieve the responsibility for reporting to ASU or OPR, as defined in the MAOP.

(3) Any person who knowingly, willfully, or negligently discloses information to unauthorized persons will be subject to the appropriate penalties and sanctions under the law (i.e., Privacy Act, Computer Fraud and Abuse Act, National Security Act, or appropriate espionage statutes).

(4) Non-FBI employees who violate this policy are subject to having their access to FBI ADPT systems and facilities terminated.

EFFECTIVE: 07/26/95

35-11 REGULATIONS/LAWS GOVERNING ADPT SECURITY (See MIOG, Part II, 35-2, 35-5.)

(1) Title 5, U.S. Code, 552a, "Privacy Act of 1974," (Public Law 93-579), December 31, 1974

(2) Title 5, Code of Federal Regulations (CFR), Part 930, Subpart C, "Employees Responsible for the Management of Use of Federal Computer Systems"

(3) Title 31, U.S. Code, 1105, 1113, 3512, "Federal Managers' Financial Integrity Act of 1982," (Public Law 97-255), September 8, 1982 (FMFIA)

(4) Title 18, U.S. Code, 1030, "Computer Fraud and Abuse Act of 1986," (Public Law 99-474), October 16, 1986

(5) Title 18, U.S. Code, 2701, "Electronic Communications Privacy Act of 1986," (Public Law 99-508), October 21, 1986

(6) Title 40, U.S. Code, 759, "Computer Security Act of 1987" (Public Law 100-235), January 8, 1988

(7) Title 41, CFR, 201, Federal Information Resources Management Regulation (FIRMR)

(8) Title 44, U.S. Code, 3501-3520, "The Paperwork Reduction Act of 1980" (Public Law 96-511), December 11, 1980

(9) Department of Justice (DOJ) Order 2640.2C, "Telecommunications and Automated Information Systems Security," June 25, 1993

(10) Department of Justice (DOJ) Order 2830.1D, "Automated Information Systems Policies," October 3, 1986

(11) Department of Justice, "Simplified Risk Analysis Guidelines (SRAG)," May 18, 1990

(12) Director of Central Intelligence Directive (DCID) No. 1/14, "Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information," January 22, 1992

(13) Director of Central Intelligence Directive (DCID) No.

1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks," July 19, 1988

(14) Director of Central Intelligence Directive (DCID) No. 1/21, "Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)," January 30, 1994

(15) Executive Order 12958 (E.O. 12958), "National Security Information," April 20, 1995

(16) Federal Information Processing Standards Publication, FIPS PUB 65, "Guidelines for Automatic Data Processing Risk Analysis"

(17) Federal Information Processing Standards Publication, FIPS PUB 87, "Guidelines for ADP Contingency Planning"

(18) Federal Information Processing Standards Publication, FIPS PUB 112, "Password Usage"

(19) Government Accounting Office (GAO) "Policy and Procedures Manual for Guidance of Federal Agencies - Title II - Accounting"

(20) National Security Council/Policy Coordinating Committee, National Security Directive 42 (NSD 42), "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990

(21) National Telecommunications and Information Systems Security Directive (NTISSD) No. 500, "Information Systems Security (INFOSEC) Education, Training, and Awareness," February 25, 1993

(22) National Telecommunications and Information Systems Security Instruction (NTISSI) No. 7000, "Tempest Countermeasures for Facilities," November 29, 1993

(23) National Telecommunications and Information Systems Security Policy (NTISSP) No. 200, "National Policy on Controlled Access Protection," July 15, 1987

(24) National Telecommunications and Information Systems Security Policy (NTISSP) No. 300, "National Policy on Control of Compromising Emanations," November 29, 1993

(25) NIST Special Publication 500-174, "Guide for

Selecting Automated Risk Analysis Tools," October 1989

(26) Office of Management and Budget (OMB) Circular A-123, "Internal Control Systems," August 4, 1986

(27) Office of Management and Budget (OMB) Circular A-127, "Financial Management Systems," December 19, 1984

(28) Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Sources," June 25, 1993

(29) Office of Management and Budget (OMB) Bulletin 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information"

(30) Department of Defense (DoD) 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria"

(31) National Computer Security Center Technical Guide 005 (NSC-TG-005), "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria"

(32) National Computer Security Information Memorandum (NACSIM) 5203, "Guidelines for Facility Design and Red/Black Installation (U)," June 30, 1982

(33) Appendix B to NACSIM 5204, "NSA Specifications for RF Shielded Enclosures for Communications Equipment General Specifications (U)"

EFFECTIVE: 07/26/95

35-12 GLOSSARY OF TERMS (See MIOG, Part II, 35-3.)

(1) Access - the capability and opportunity to gain knowledge of, or to alter information or materials, including the ability and means to communicate with (i.e., input or receive output), or otherwise make use of any information, resource, or component in a computer system.

(2) Access Control - the process of limiting access to the resources of a system to only authorized persons, programs,

processes, or other systems. Synonymous with controlled access and limited access.

(3) Accreditation - the official management authorization for operation of an ADPT system which provides a formal declaration by an accrediting authority that a computer system is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is based on the certification process, as well as other management considerations. An accreditation statement affixes security responsibility with the accrediting authority and shows that proper care has been taken for security.

(4) Accrediting Authority - the official who has the authority to decide on accepting the security safeguards prescribed for a computer system or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The Senior Executive Service personnel designated by the Director, FBI, are the authorized accrediting authorities.

(5) Automated Data Processing Telecommunications (ADPT) System - an assembly of hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control information in an automated fashion. An ADPT system must be under the same direct management control with essentially the same function, reside in the same environment and have the same characteristics and security needs. Examples of ADPT systems include, but are not limited to: mainframe, minicomputer, microcomputer, local and wide area networks, connectivity and control hardware/firmware and application systems.

(6) ADPT Security - measures or controls that safeguard or protect an ADPT system against unauthorized (accidental or intentional) disclosure, modification, destruction of ADPT system and data, or denial of service. ADPT system security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at all computer facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the ADPT and for the data contained in the system.

(7) Authorization - the privileges and permissions granted to an individual by a designated official to access or use a program, process, information, or system. These privileges are based on the individual's clearance and need-to-know.

(8) Authorized Person - a person who has the need-to-know for classified or sensitive information in the performance of official duties and who has been granted a personnel security clearance or authorized access at the required level. The responsibility for determining whether a prospective recipient is an AUTHORIZED PERSON rests with the person who has possession, knowledge, or control of the classified or sensitive information involved, and not with the prospective recipient.

(9) Audit Trail - a chronological record of system activities that enables the reconstruction and examination of the sequences of events and/or changes in an event.

(10) Authenticate - the process to verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

(11) Availability - the property of being accessible and usable upon demand by an authorized entity. Required ADPT services must remain available to authorized users operating within the same security constraints that make these services unavailable to unauthorized users.

(12) Certification - the comprehensive security test and evaluation of the technical and nontechnical security features of a computer system and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

(13) Classified - any information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure and is so designated.

(14) Clearing - the process of removing information recorded on an ADPT storage media and nonvolatile memory devices. Clearing cannot be used to downgrade/declassify ADPT storage media or nonvolatile memory. Clearing can be performed in the field using FBIHQ-approved means and is used when the microcomputer and ADP storage media remain in FBI control.

(15) Compartmented Security Mode - an operational method where each user with direct or indirect individual access to a computer system, its peripherals, and remote terminals or hosts meets

all the following criteria:

(a) a valid personnel security clearance for the most restricted information in the computer system.

(b) formal access approval, and has signed nondisclosure agreements, for that information to which that user is to have access.

(c) a valid need-to-know for that information to which that user is to have access.

(16) Communications Security (COMSEC) - the protective measures taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such communication. Communications security includes crypto security, transmission security, and physical security of COMSEC material.

(17) Compromise - the disclosure of classified or sensitive information to persons not authorized access or having a need-to-know.

(18) Compromising Emanations - unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment.

(19) Confidentiality - sensitive data that are held in confidence and are protected from unauthorized disclosure. FBI ADPT systems support a range of unclassified, sensitive and classified National Security Information, up to and including TOP SECRET code word material.

(20) Configuration Management (CM) - an approach for specifying, documenting, controlling, and maintaining the visibility and accountability of all appropriate hardware, software, firmware, communications interfaces, operating procedures, installation structures, and all changes thereto.

(21) Contingency Plan - an emergency response plan, backup operations plan, and post-disaster recovery plan, maintained by an activity as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Synonymous with disaster plan and emergency plan.

(22) Declassification - a formal statement that a microcomputer system or its media is UNCLASSIFIED.

(23) Dedicated Security Mode - an operational method when each user with direct or indirect individual access to a computer system, its peripherals, and remote terminals or hosts meets all the following criteria:

(a) a valid personnel security clearance for all information on the system.

(b) a valid need-to-know for all information contained within the system.

(c) for classified systems, formal access approval, and signed nondisclosure agreements for all the information stored and/or processed (to include all compartments, subcompartments, and/or special access programs).

(24) Dedicated System - a system that is specifically and exclusively dedicated to and controlled for a specific mission, either for full-time operation or a specified period of time.

(25) Denial of Service (DOS) - the prevention of authorized access to resources or the delaying of time-critical operations. DOS refers to the inability of an ADPT system or any essential part to perform its designated mission, either by loss of, or degradation of operational capability.

(26) Department of Defense (DoD) Trusted Computer System Evaluation Criteria - a document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built in the design and evaluation of systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store sensitive or classified data. This document is also referred to as the "Orange Book."

(27) Encryption - the process of transforming data to an unintelligible form to conceal its meaning in such a way that the original data cannot be obtained without using the inverse decryption process.

(28) Environment - the aggregate of external procedures, conditions, and objects that affect the development, operation, and

maintenance of a system.

(29) FBINET - The FBI Network that provides secure communications for the FBI Data Network supporting classified automated applications up to the SECRET noncode word level.

(30) Identification - the process that enables recognition of an entity by a system, generally by the use of unique machine readable user names.

(31) IISNET - the Intelligence Information System Network that provides secure communications for the FBI Data Network supporting classified automated applications to include TOP SECRET code word material.

(32) Individual Accountability - the ability to associate positively the identity of a user with the time, method, and degree of access to a system.

(33) Industrial Security - the management, control and safeguard of FBI information entrusted to contractors.

(34) Information Security - the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

(35) Integrity - computerized data that is the same as those in the source documents and has not been exposed to accidental or malicious alteration or destruction. The information processing must ensure the data is accurate, timely, and complete to support the FBI's investigative, law enforcement, and administrative support requirements. Inaccurate data could lead to uninformed decisions and adversely impact investigations.

(36) Interconnected System - an approach in which the network is treated as an interconnection of separately created, managed, and accredited computer systems.

(37) Label - the marking of an item of information that reflects its security classification. An internal label is the marking of an item of information that reflects the classification of that item within the confines of the medium containing the information. An external label is a visible or readable marking on

the outside of the medium or its cover that reflects the classification of the information resident within that particular medium.

(38) Least Privilege - the principle that requires each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

(39) Microprocessor - a semiconductor central processing unit contained on a single integrated circuit chip.

(40) Mode of Operation - a description of the conditions under which a computer system functions, based on the sensitivity of data processed and the clearance levels and authorizations of the users.

(41) Multilevel Security Mode - an operational method where each user with direct or indirect individual access to a computer system, its peripherals, and remote terminals or hosts meets all the following criteria:

(a) some users do not have a valid personnel security clearance for all the information processed in the computer system.

(b) all users have the proper clearance and have the appropriate formal access approval for that information to which they have access.

(c) all users have a valid need-to-know for that information to which they have access.

(42) Need-to-Know - a determination by the owner of sensitive and/or classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the information in order to perform tasks or services essential to carry out official duties.

(43) Nonvolatile Memory Units - devices which continue to retain their contents when power to the unit is turned off (e.g., bubble memory, Read Only Memory - ROM).

(44) Overwrite Procedure - process which removes or destroys data recorded on a computer storage medium by writing

patterns of data over, or on top of, the data stored on the medium.

(45) Password - a protected and private character string used to authenticate.

(46) Personnel Security Clearance - an administrative determination, in compliance with Executive Order 10450, that an individual is eligible from a security point of view for access to classified information of the same or lower category as the level of the personnel clearance being granted.

(47) Personnel Security - the procedures established to ensure that all personnel who have access to any sensitive information have all required authorities as well as all appropriate clearances.

(48) Physical Security - the application of physical barriers and control procedures as preventative measures or countermeasures against threats to resources and information.

(49) Purge - the removal of data from computer system storage devices in such a way that there is assurance, proportional to the sensitivity of the data, that the data cannot be reconstructed.

(50) Residual Risk - the portion of risk that remains after security measures have been applied.

(51) Risk Analysis - the process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of the risk management process.

(52) Risk Management - the total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, and effectiveness reviews.

(53) SAMNET - the SAMNET is the FBI's Command and Control Network which provides for distribution between FBI divisions of classified administrative narrative traffic to include the TOP SECRET code word material.

(54) Sanitization - the technical elimination of all information from ADPT storage media and nonvolatile memory devices so they can be formally certified as declassified by appropriate authorities.

(55) Secure Configuration Control - the set of procedures

appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that changes will not lead to violations of the system's security policy.

(56) Security Countermeasures - the protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include, but are not necessarily limited to: hardware and software security features; operating procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices. Also called safeguards or security controls.

(57) Security Requirements - types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policies.

(58) Security Specifications - a detailed description of the security countermeasures/safeguards required to protect a system.

(59) Security Violation - an event which may result in disclosure of sensitive or classified information to unauthorized individuals, or that results in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss or theft of any computer system media.

(60) Sensitive but Unclassified Information - refer to Sensitive Information.

(61) Sensitive Compartmented Information (SCI) - classified information about or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems established by the Director, Central Intelligence (DCI).

(62) Sensitive Compartmented Information Facility (SCIF) - an accredited area, room, group of rooms or installation where SCI may be stored, used, discussed, and/or electronically processed.

(63) Sensitive Information - information that requires protection due to the risk or magnitude of loss or harm that could result from inadvertent or deliberate disclosure, modification and/or destruction of the information. The term includes information, the improper use or disclosure of which could adversely affect the ability of the FBI to accomplish its mission; information that is investigative in nature; grand jury information subject to the Federal

Rules of Criminal Procedure, Rule 6(e), Grand Jury Secrecy of Proceedings and Disclosure; proprietary information; records about individuals requiring protection under the Privacy Act; information not releasable under the Freedom of Information Act; and information which could be manipulated for personal profit or to hide the unauthorized use of money, equipment, or privileges. Also referred to as Sensitive but Unclassified Information and Limited Official Use Information.

(64) Standard Security Procedures - step-by-step security instructions tailored to users and operators of computer systems which process sensitive or classified information.

(65) Standalone System - a single user system not connected to any other systems.

(66) System High Security Mode - an operational method where each user with direct or indirect individual access to a computer system, its peripherals, and remote terminals or hosts meets all the following criteria:

(a) a valid personnel security clearance for all information on the computer system.

(b) a valid need-to-know for some of the information contained within the system.

(c) for classified systems, formal access approval, and signed nondisclosure agreements for all the information stored and/or processed (to include all compartments, subcompartments, and/or special access programs).

(67) System Integrity - the quality that a system has when it performs its intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

(68) Telecommunications - the preparation, transmission, communication, or related processing of information (i.e., writing, images, sounds or other data) by electrical, electromagnetic, electromechanical, electrooptical, or electronic means.

(69) TEMPEST - short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. (See Compromising Emanations.)

(70) Threat - the means through which a weakness can be exploited to adversely affect an ADPT system, facility, network, or operation. Threats can be categorized as human or environmental in origin and include sabotage, espionage, natural disasters, data disclosure, data destruction, hardware/software failure, etc.

(71) Trusted Computing Base (TCB) - totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. The ability of a trusted computing base to enforce correctly a unified security policy depends on the correctness of the mechanisms within the trusted computing base, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy.

(72) Volatile Memory Units - devices which do not retain their contents when the power to the unit is turned off (e.g., Random Access Memory - RAM). Volatile memory units become UNCLASSIFIED when the system is turned off.

(73) Vulnerability - a potential weakness in an existing or planned security control environment whose exploitation may impact the confidentiality, integrity, and/or availability of a specific resource or mission.

EFFECTIVE: 07/26/95

35-13 COMPUTER SECURITY AWARENESS CHECKLIST

OFFICIAL BUSINESS ONLY - FBI computer systems, both mainframes and microcomputers, are for official business only. You have NO EXPECTATION OF PRIVACY in their use.

AUDIT OF USER ACTIVITIES - All systems transactions are subject to recording and routine review for inappropriate or illegal activity conducted.

SANCTIONS - A violation of security requirements could result in termination of system access privileges and serious disciplinary action, possibly removal. In addition, Title 18, USC, Section 1030 provides criminal penalties for any person illegally accessing a government-owned or -operated computer.

CLASSIFICATION - A microcomputer and associated magnetic media is classified at the highest level of information that has been entered into, stored on, or produced by the system unless the system can be appropriately declassified. The microcomputer must be labeled, secured, and operated commensurate with its classification level. FBI PORTABLE microcomputers |are authorized| to process classified information |up to and including Secret/Collateral within the U.S. and its territories and can be connected to the FBI Secure Network (FBINET). The processing of Top Secret and SCI information is not authorized on portable microcomputers without written authorization |by the FBI's Security Programs Manager (SPM). (See MIOG, Part II, 35-9.4.9.)

LABELS -|Removable ADPT| storage media must be marked with a classification and a data descriptor label. |Microcomputers| with nonremovable |ADPT| storage devices must conspicuously display a classification and a data descriptor label on the unit that contains the magnetic |ADPT| storage device. |Portable microcomputers are exempt from this provision.| (See MIOG, Part II, 35-9.4.10.)

STORAGE - All |ADPT| storage media must be labeled and secured in accordance with existing policies.

PROTECT AGAINST DISASTER - Back up all your data files on a regular basis, according to your division's "END-USER AUTOMATED DATA PROCESSING CONTINGENCY PLAN."

DOWNGRADING/DECLASSIFYING -|ADPT| storage media (operative and inoperative, removable and nonremovable) and nonvolatile memory devices may NEVER be downgraded or declassified in the field.

EQUIPMENT AND MEDIA DISPOSAL - Microcomputer equipment which has processed sensitive or classified information may not be released from FBI control until the equipment is sanitized and declassified. When inoperable, diskettes, tape cartridges, printouts, ribbons, and similar items used to process sensitive or classified information must be destroyed as classified trash. When inoperable, hard disks used to process sensitive or classified information must be sent to FBIHQ for proper disposal. (See MIOG, Part II, 35-9.4.14.)

MAINTENANCE - All maintenance must be performed only by properly cleared persons and must be supervised by FBI personnel knowledgeable in the operation of microcomputers. Vendor diagnostic software used on any FBI microcomputer may not be removed from FBI-controlled environment. All electronic, storage, and memory devices associated with FBI microcomputers must remain in FBI-controlled space and may

never be returned to the vendor for "trade-in" or credit purposes. |ADPT|storage media and microcomputers with nonremovable|ADPT|storage media must be transferred for off-site maintenance only through FBIHQ control channels. (See MIOG, Part II, 35-9.4.5.)

PHYSICAL CONTROL - FBI microcomputers which process sensitive or classified information must be operated only in FBI-controlled space and under the direct supervision of authorized persons. When not under the direct supervision of an authorized person either during or outside regular working hours, FBI microcomputers must be: turned off; diskettes, tapes, removable hard disks, and printer ribbons must be labeled, removed, and secured. Microcomputers with nonremovable |ADPT|storage media and nonvolatile memory devices operated in areas that are not|staffed|24 hours a day (e.g., resident agencies, off-sites) must not be used to process or store classified information. To the extent possible, PORTABLE microcomputers should be kept in the possession of the individual to whom they are issued or charged out. PORTABLE computers which must be left unattended for any amount of time must be properly secured. (See MIOG, Part II, 35-9.4.6.)

SOFTWARE CONTROLS - All software used on FBI microcomputers must be obtained through either: the Operations Management Section, Information Resources Division, FBIHQ, or appropriate FBI procurement channels.

INTRODUCTION OF NON-FBI DATA - Introduction of non-FBI data (e.g., transcripts from United States Attorneys, information from Joint Task Force agencies) must be approved in writing by the SAC as an operational necessity, and all magnetic media must be scanned for viruses prior to use. (See MIOG, Part II, 35-9.4.4.)

SENSITIVE COMPARTMENTED INFORMATION (SCI) - FBI ADPT operations involving SCI must be conducted in accordance with the provisions of Director of Central Intelligence Directive (DCID) No. 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Systems and Networks."

TEMPEST - A microcomputer used to process classified information must meet national TEMPEST standards. FBIHQ provides TEMPEST certifications. Any change to the approved configuration, including internal components or external devices, or relocation of the microcomputer invalidates the TEMPEST certification.

TELECOMMUNICATIONS - Unencrypted dial-up access to FBI information systems or networks is prohibited. FBI microcomputers must not be connected to any non-FBI network, public or private. All

microcomputers connected to the Integrated Digital Communications System (IDCS) (formerly the Computer Applications Communications Network (CACN)), are considered classified and must be appropriately labeled. Exceptions may only by granted by the FBIHQ ADPT Security Officer. (See MIOG, Part II, 35-9.4.8.)

BULLETIN BOARDS - A comprehensive program of monitoring electronic bulletin boards for criminal or intelligence purposes is prohibited. Any access to non-FBI electronic bulletin boards is severely restricted. (See MIOG, Part II, 35-9.4.8.)

MAINFRAME ACCESSOR IDs AND PASSWORDS - Each user is assigned a unique accessor ID for identification and a unique password to be used for authentication. Accessor IDs may be publicly known, passwords must be kept secret. It is your responsibility to protect your password. Passwords serve as an "electronic signature" on all system transactions for which they are used. You will be held responsible if someone else uses your password in connection with a system transaction.

Your password is for your use only. Lending it to someone else is a security violation and may result in disciplinary action against both parties.

Never disclose your password to anyone. Memorize it; do not put it in writing. Safeguard it. Your password is the key to one of the FBI's most valuable resources.

If you forget your password, notify your Computer Specialist. Your old password will be deleted from the system and a new one issued.

Immediately following a suspected or known compromise of a system password, a new password will be issued and the compromised password deleted from the system.

When a system user no longer needs access, the password will be removed from the system.

If you leave the terminal unattended for any reason, log off. An unattended terminal is vulnerable to masquerading. Any user signed on to a terminal which has been inactive for a period of 30 minutes will be automatically signed off. You must reidentify yourself by reestablishing the session. (See MIOG, Part II, 35-9.4.2.)

REPORT SECURITY VIOLATIONS - If you become aware of any violation of these requirements or suspect that your password may have been used by someone else, it is your responsibility to report that information immediately to your respective Division Security Officer, field office or FBIHQ Computer Specialist.

If you have any questions about the proper operation or security of computer systems entrusted to you, contact a field office or FBIHQ Computer Specialist or Division Security Officer.

EFFECTIVE: 08/18/97

35-13.1 Notice of Responsibilities and Computer Security Awareness Certification (See MIOG, Part II, 35-8.3)

You have been entrusted with the management, operation, or use of a Federal Bureau of Investigation (FBI) computer system processing sensitive and/or classified information. Both you and the FBI have responsibility pursuant to the Computer Security Act of 1987 to protect sensitive information and under 28 CFR, Part 17, to protect classified information. Specific responsibilities are set forth in Manual of Investigative Operations and Guidelines (MIOG), Part II, Section 16-18, "FBI MICROCOMPUTER POLICY;" MIOG, Part II, Section 35, "FBI AUTOMATED DATA PROCESSING AND TELECOMMUNICATIONS SECURITY POLICY;" and in MIOG, Part II, Section 26, "CLASSIFIED NATIONAL SECURITY INFORMATION AND MATERIAL." At a minimum, you must follow the attached security awareness checklist as a basic guide and reminder of your responsibilities to protect the information processed and/or stored in the computer system(s) entrusted to you. For additional information about computer security, contact the field office or FBIHQ Computer Specialist or Division Security Officer.

I certify that I have read, understand, and shall comply with the practices and requirements of the preceding notice and the attached FBI Computer Security Awareness Checklist.

_____ _____

Signature Date

_____ _____

35-13.2 Nondisclosure Agreement for Joint Task Force/Contractor Members (FD-868) (See MIOG, Part II, 35-9.4.1.)

FD-868 (8-19-97)

(FBI SEAL)

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

NONDISCLOSURE AGREEMENT FOR JOINT TASK FORCE/CONTRACTOR MEMBERS
AN AGREEMENT BETWEEN _____ AND THE FBI
(Name of Individual-Printed or Typed)

As consideration for assignment in the Federal Bureau of Investigation (FBI), United States Department of Justice, and as a condition for continued assignment, I hereby declare that I intend to be governed by and I will comply with the following provisions:

1. That I am hereby advised and I understand Federal Law, including statutes, regulations issued by the Attorney General and Orders of the President of the United States, prohibit loss, misuse or unauthorized disclosure or production of information in the files of the FBI.

2. I understand that unauthorized disclosure of information in the files of the FBI or information I may acquire as a Task Force/Contractor employee of the FBI could result in impairment of national security, place human life in jeopardy, or result in denial of due process to a person or persons who are subjects of an FBI investigation, or prevent the FBI from effectively discharging its responsibilities. I understand the need for this secrecy agreement; therefore, as consideration for assignment, I agree that I will never divulge, publish, or reveal either by word or conduct, or by other means of disclosure to any unauthorized recipient without official

written authorization by the Director of the FBI or his delegate, any information from the investigatory files of the FBI or any information relating to material contained in the files, or disclose any information or produce any material acquired as a part of the performance of my official duties or because of my official status. The burden is on me to determine, prior to disclosure, whether information may be disclosed and in this regard I agree to request approval of the Director of the FBI in each such instance by presenting the full text of my proposed disclosure in writing to the Director of the FBI at least thirty (30) days prior to disclosure. I understand that this agreement is not intended to apply to information which has been placed in the public domain or to prevent me from writing or speaking about the FBI, but it is intended to prevent disclosure of information where disclosure would be contrary to the law, regulation, or public policy. I agree the Director of the FBI is in a better position than I to make that determination.

3. I agree that all information acquired by me in connection with my duties while on assignment with the FBI and all official material to which I have access remains the property of the United States of America, and I will surrender upon demand by the Director of the FBI or his delegate, or upon separation from the FBI, any material relating to such information or property in my possession. I also agree assignment to the United States of any profits resulting from the publication of information in breach of this agreement.

4. I understand that obtaining information under false pretenses or any unauthorized disclosure may be a violation of Federal law and prosecuted as a criminal offense and, in addition to this agreement, may be enforced by means of an injunction or other civil remedy. I also understand that the use of the FBI network and its automated information systems, i.e., the Automated Case Support (ACS) System, to access records other than in furtherance of authorized responsibilities will be viewed as obtaining information under false pretenses and may be in violation of the Privacy Act.

5. I agree that all the information that I will access will be for the sole purpose of authorized and lawful purposes in furtherance of the responsibilities of the particular Joint Task Force or contract under which the user is being provided access. (JTF/Contract _____ _____)

I accept the above provisions as conditions for my assignment and continued assignment in the FBI. I agree to comply with these provisions both during my assignment in the FBI and following termination of such assignment. I have read this Agreement carefully

and my questions, if any, have been answered.

_____
(Signature)

_____
(Type or Print Name)

Witnessed and accepted in behalf of the Director FBI on

_____, _____, by _____
(Date) (Year) (Signature)

EFFECTIVE: 08/19/97